BELKIN®

Server console seriale OmniView®

Manuale utente

F1DP116Sea

Table of Contents

Descrizione generale del prodotto....1
Introduzione 1
Contenuto della confezione 1
Caratteristiche del server console....2
Requisiti dell'apparecchiatura....3
Requisiti di sistema 3
Diagrammi di visualizzazione dell'unità....4
Indicatori LED, pulsante e connettori....5
Specifiche 6

Installazione locale....7
Installazione su scrivania o su rack....8
Collegamento dei dispositivi di destinazione al server console....9

Configurazione della rete 10
Interfaccia browser web....10
Assegnazione di un indirizzo IP dalla porta della console VT-100 (Console, Telnet, SSH). 13
Interfaccia di gestione basata sul web....16

Impostazioni di rete 18
Configurazione IP....18
Filtraggio IP 19
Configurazione del server web....21
Locale 21
RADIUS e locale 21
DNS dinamico 22
RADIUS 23
Configurazione del server RADIUS 24
HTTPS/SSL 24

Porte seriali....25
Configurazione 25
Porta di autenticazione 25
Abilitazione / disabilitazione porta 26
Titolo della porta 26
Modalità di funzionamento 27
Modalità "Console-Server" 27
Modalità "Terminal server" 28
Modalità "modem dial in" 29
Parametri della porta seriale 29
Registrazione della porta 30
Funzione break 31
Connessione 31
Applet Telnet Java 32
Modalità da seriale a seriale....34

Table of Contents

Stato e registrazione del sistema **37**
Stato del sistema 37
Registrazione del sistema 37

Amministrazione del sistema **39**
Amministrazione dell'utente 39
Aggiunta di un utente 39
Eliminazione di un utente 40
Modifica dell'elenco "Access Control List" (ACL) 41
Modifica della password 42
Data e ora (NTP) 42
Aggiornamento del firmware 43
Aggiornamento dall' interfaccia web 43
Certificato SSL 44
Certificato HTTP sicuro 45
Ripristino delle impostazioni predefinite 49
Riavvio 49

Dati tecnici **50**
Impostazioni predefinite 50

Allegato A: Adattatori **51**

Allegato B: Connettori Ethernet (RJ45) **54**
Cavo Ethernet con connettore RJ45 standard 54

Allegato C: Numeri di porta TCP/UDP nota **55**

Allegato D: Glossario protocollo **56**

Allegato E: Creazione di file CA **58**

Informazioni **60**

Introduzione

Grazie per aver acquistato il server console seriale OmniView Belkin (Server console). Questo dispositivo permette agli amministratori di monitorare e controllare server, router, switch e altri dispositivi seriali da qualsiasi punto all' interno della rete TCP/IP, sia via Internet sia con connessioni via modem dial up, persino quando il server non è raggiungibile dalla rete.

Il server console offre:

- Protezione del percorso dati mediante SSH o web/SSL
- Una interfaccia protetta e crittografata mediante SSL (HTTPS)
- La crittografia SSHv2, per mantenere le password di accesso al server fuori dalla portata di eventuali hacker
- Compatibilità con tutti i maggiori client SSH
- Accesso sicuro da qualsiasi browser con abilitazione Java
- Connessioni alle porte seriali/console mediante cavi standard CAT5, eliminando i problemi della lunghezza dei cavi

Contenuto della confezione

1	server console seriale OmniView
1	adattatore di corrente alternata
5	kit con adattatori seriale/RJ45 (5 pezzi)
1	adattatore per porta seriale console locale
1	cavo CAT5 RJ45/RJ45 da 1,8 m
1	guida di installazione rapida
1	manuale d'uso su CD-ROM
1	staffe per montaggio su rack con viti
1	set di piedini

Caratteristiche del server console

- **Gestione in banda e fuori banda**
  Le soluzioni per la gestione delle porte della console offrono un accesso remoto, affidabile e sicuro alle porte seriali/console mediante le opzioni per la connettività delle reti in banda e fuori banda, quali l'accesso al terminale seriale e il modem dial-up.
- **Possibilità di gestire i dispositivi/server di rete in modo centralizzato, remoto e sicuro**
  Le soluzioni affidabili per la gestione delle porte della console permettono di criptare dati sensibili usando dei protocolli già sperimentati quali SSH/v2 e SSL.
- **Gestione di vari dispositivi**
  La semplice emulazione del terminale ASCII o VT-100 non basta a gestire questa vasta gamma di tipi di dispositivi. I centri dati attuali contengono una vasta gamma di server, quali UNIX®, Linux®, RISC, mainframe e Windows®, così come altri dispositivi con gestione seriale come router, gateway, firewall, PBX, UPS, SAN e dispositivi NAS e prese multiple intelligenti.
- **Monitoraggio attivo e messaggi di avviso per supportare la diagnostica del sistema**
  Le applicazioni e persino i sistemi operativi inviano messaggi al sistema della console. Questi messaggi contengono informazioni relative ad errori e messaggi di panico che spesso precedono un crash del sistema. A differenza dei terminal server, i console port server memorizzano questi messaggi in tempo reale e permettono agli amministratori di sfogliare e ricercare tali dati successivamente. Inoltre, in caso di eventi critici, inviano dei messaggi di allerta via e-mail agli amministratori IT.
- **Dispositivo di controllo della corrente sicuro e remoto**
  Questo dispositivo funziona via porta seriale e funge da comando principale per le prese multiple, può infatti controllare varie prese multiple (fino a 15).
- **Modalità da seriale a seriale**
  Questa funzione permette al dispositivo di incorporarsi ad un convertitore per reti di terminali per avere delle porte VGA e per la tastiera locali, oppure per collegare le porte VGA/tastiera allo switch KVM per rafforzarne l'amministrazione.
- **Elenchi degli accessi alle porte per gli utenti**
  Grazie all'elenco "Access Control List" (ACL) dell'amministrazione utente, tutti gli utenti ad eccezione degli **amministratori** sono autorizzati ad usare un set di porte seriali. Gli utenti possono accedere e apportare delle modifiche alla configurazione delle porte seriali autorizzate che sono state loro assegnate da un account **amministratore**.

Requisiti dell'apparecchiatura

- Kit per la connettività universale (incluso)
- Cavo CAT5 RJ45/RJ45 (incluso)

Requisiti di sistema

Browser web

Browser		
Sistema operativo	Microsoft Internet Explorer versione 6.0 SP1 e successive	Firefox versione 2.0 e successive
Windows 2000 SP2	Sì	Sì
Windows Server 2003	Sì	Sì
Windows XP	Sì	Sì
Windows Vista	Sì	Sì
Red Hat Linux 3 e 4	No	Sì
Sun Solaris 9 e 10	No	Sì
Novell SUSE Linux 9 e 10	No	Sì
Fedora Core 4 e 5	No	Sì
Mac OS X 10.4+	No	Sì

Plug-In Java

L'interfaccia web del server console richiede l'installazione di JRE (Java Runtime Environment) v6.0 o successive. Il software Java più recente può essere scaricato dal sito: http://www.java.com/en/download/manual.jsp.

Diagrammi di visualizzazione dell'unità

Pannello anteriore/posteriore

Fig. 1 Vista anteriore

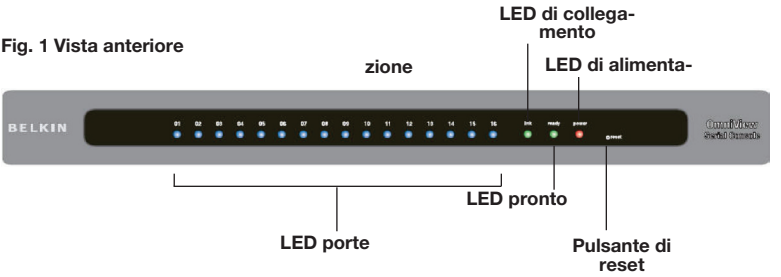
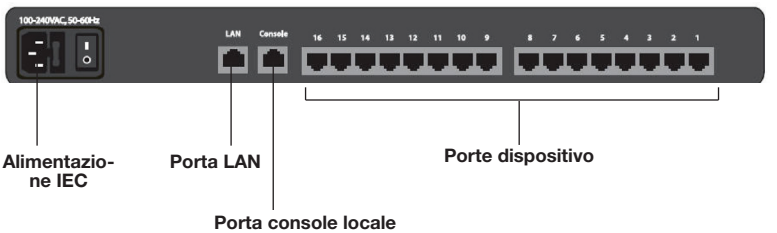


Fig. 2 Vista posteriore



Indicatori LED, pulsante e connettori

LED	Indicazione
Alimentazione	**Rosso –** Indicatore di alimentazione *ACCESO: Il dispositivo è alimentato*
Collegamento	**Collegamento Ethernet/Attività/10/100 Mbps:** **Arancione –** La connessione Ethernet 10BaseT è stata effettuata **Verde –** La connessione Ethernet 100BaseT è stata effettuata *Lampeggiante: attività dati* *ACCESO: Nessuna attività dati e collegamento effettuato*
Pronto	**Verde** – Lampeggia una volta al secondo quando il sistema è pronto
Attività porta (un LED per porta)	**Blu** – attività traffico *ACCESO: in uso (collegamento porta effettuato correttamente)* *Lampeggiante: attività traffico sulla porta seriale*

- **Pulsante di RESET** : Per far riavviare il server console, premere il pulsante e rilasciarlo velocemente. Per ripristinare le impostazioni predefinite dell'unità, premere e tenere premuto il pulsante "Reset" per più di cinque secondi.
- Connettore **ETHERNET** RJ45: Interfaccia Ethernet
- Connettore **CONSOLE** RJ45: Interfaccia console locale RS232
- **Altri connettori**RJ45: porte seriali

Specifiche

Funzione	Specifiche
Generale	**LED** Power (Alimentazione, rosso) Ready (Pronto, verde, generalmente lampeggiante), Collegamento/Attività/10/100 Mbps (Ethernet arancione: 10 Mbps, verde: 100 Mbps)
	Activity (Attività, blu per ogni porta seriale)
	Premere il pulsante per fare il reset, oppure per ripristinare le impostazioni predefinite
	RTC (orologio in tempo reale)
Interfaccia seriale	16 porte (F1DP116S)
	Modalità porta seriale (RS232)
	Connettore seriale (RJ45)
	Trasmissione in baud (da 300 a 115200)
	Controllo di flusso (Nessuno, RTS/CTS, Xon/Xoff)
Interfaccia LAN	Connettore RJ45
	IEEE 802.3 - 10/100BaseT
	Rilevamento automatico, selezione full e half duplex
Funzione porta	**Modalità di funzionamento**
	Console server
	Terminal server
	Modem dial-in
	Seriale/seriale (solo sulla porta 16)
Protocolli	TCP, UDP, IP, ARP, ICMP, HTTP/HTTPS, Telnet, DHCP/BOOTP, PPP,
	SMTP, DNS, NTP
	DNS dinamico
Operazioni di protocollo relativo	Intervallo di inattività TCP (TCP keep-alive time)
	Intervallo di inattività seriale
	Monitoraggio porta
Protezione	Accesso con password
	Filtraggio IP
	SSHv2
	HTTPS/SSL
Autenticazione	Database utente locale
	PAP/CHAP (per modem dial-in)
	RADIUS
Gestione	Console locale (menu o linea di comando)
	SSH, telnet
	Pagine web (HTTP/HTTPS)
	Aggiornamento firmware via interfaccia web
	Memorizzazione e registrazione delle porte
	Display dello stato del sistema ricco di funzionalità
Alimentazione e ambiente	Ingresso c.a. (100 ~ 240 V CA, 50 ~ 60 Hz)
	Temperatura di funzionamento: -10° a 80° C
	Temperatura di immagazzinaggio: -20° a 85° C
	Umidità: 0-90% non condensante
Certificazioni	CE, FCC
	UL
Meccanica	Montabile su rack da 1U 19˝
	Dimensioni (cm): 43,2 x 18,0 x 4,2

Nota bene: le specifiche sono soggette a variazioni senza obbligo di preavviso.

Posizionamento del server console:
il telaio del server console è stato progettato per essere usato come unità indipendente o montato su rack. Il server console può essere montato su un rack standard da 19 pollici utilizzando le staffe di montaggio e le viti comprese nella confezione.

Per decidere dove posizionare il server console, è necessario prendere in considerazione i seguenti aspetti:

- la posizione dei propri dispositivi di destinazione rispetto alla console
- la lunghezza dei cavi utilizzati per collegare i dispositivi alla console
- la fonte di alimentazione - Collegarlo solamente alla fonte di alimentazione indicata sull'unità. Quando varie componenti elettriche sono installate su rack, assicurarsi che il carico totale non superi quello della capacità del circuito.

Lunghezza dei cavi (CAT5)
I segnali binari seriali (RS232) si trasmettono in maniera eccellente fino a 15 metri. Superata questa distanza, le probabilità di un peggioramento del segnale aumentano. Per questo motivo, Belkin consiglia che la lunghezza del cavo UTP CAT5 tra il server console e i server collegati non superi i 15 metri.

Cavi e adattatori
Per ottenere la massima integrità del segnale con il server console, Belkin consiglia di utilizzare cavi patch Belkin di Categoria 5e, FastCAT5e oppure di Categoria 6.

Cavi patch UTP Belkin:

A3L791-XX-YYY (CAT5e)

A3L850-XX-YYY (FastCAT™ 5e)

A3L980-XX-YYY (CAT6)

Consultare pagina 54 dell'allegato B per la guida relativa ai connettori.

Adattatore seriale Belkin:

F1D120ea (RJ45F/DB9F DTE)

F1D121ea (RJ45F/DB25F DTE)

F1D122ea (RJ45F/DB25M DCE)

F1D123ea (RJ45F/DB25M DTE)

F1D124ea (RJ45F/RJ45M CISCO)

F1D120ea-8PK (Pacco da 8 del prodotto F1D120ea)

F1D124ea-8PK (Pacco da 8 del prodotto F1D124ea)

Per le illustrazioni dettagliate di tutti gli adattatori seriali, consultare pagina 51 dell'allegato A.

Installazione su scrivania o su rack

Il server console può essere collocato su una scrivania oppure montato su un rack da 19 pollici / 1 unità.

Nota bene: prima di cominciare, individuare l'indirizzo MAC e il numero di serie sul retro del server console. Questi numeri potrebbero essere necessari durante la procedura di installazione. Pertanto, è consigliabile prendere nota di questi numeri prima di montare il server console nel rack.

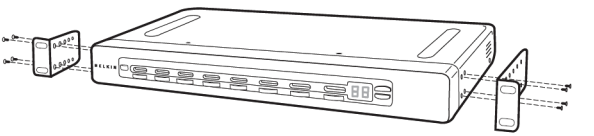
Indirizzo M**AC**	**Numero di serie**

Il server console comprende delle staffe regolabili ideali per il montaggio su rack da 19 pollici. Le staffe di montaggio sono regolabili in tre posizioni, in modo tale da permettere di far scorrere la parte anteriore del server console insieme alle estremità delle guide o di posizionarla oltre la parte anteriore delle guide. Seguire i passaggi riportati di seguito per ottenere la regolazione desiderata.

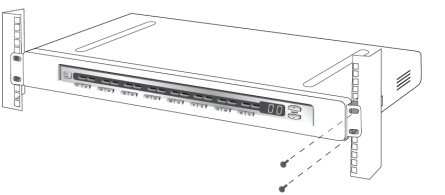
Montaggio su rack

1. Decidere quanto si vuole che il server console fuoriesca dal rack. Scegliere uno schema di foratura delle staffe.

2. Fissare la staffa sul lato del server console utilizzando le viti Phillips fornite (vedere lo schema riportato di seguito).



3. Agganciare il server console alle guide del rack e fissarlo usando le viti fornite (vedere lo schema riportato di seguito).



Il server console ora è montato correttamente sul rack e può essere collegato ai dispositivi di destinazione.

Collegamento dei dispositivi di destinazione al server console

1. Spegnere i dispositivi di destinazione che devono essere collegati al server console.
2. Collegare il cavo Ethernet fornito alla porta contrassegnata con la dicitura LAN.
3. Prendere il cavo di alimentazione fornito e collegarlo alla presa di alimentazione situata sul retro del server console. Quindi collegare l'altra estremità alla presa a muro.

Nota bene: attendere circa 100 secondi prima che il processo di riavvio del server console sia completato.

4. Scegliere una delle porte numerate sul retro del server console. Inserire un'estremità di un cavo patch UTP (4 paia, fino a 15 metri) nella porta selezionata e collegare l'altra estremità al dispositivo di destinazione. Potrebbe essere necessario aggiungere un adattatore per il dispositivo di destinazione. Per ulteriori informazioni vedere l'Allegato A a pagina 51 di questo manuale.
5. Ripetere il procedimento per ogni dispositivo di destinazione (vedere lo schema riportato di seguito).

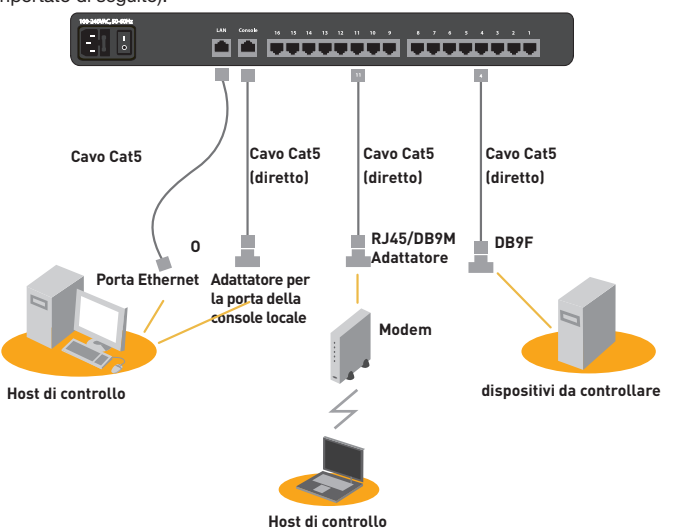


Fig. 3 Installazione dei cavi—Questo diagramma rappresenta degli esempi di connessioni cablate per vari tipi di interfacce.

Prima di collegarsi ad un dispositivo di destinazione, bisognerà configurare le impostazioni di rete. Il server console prevede due metodi di impostazione di rete: via browser web o mediante la porta della console locale.

Il server console è compatibile sia con il protocollo DHCP (Dynamic Host Configuration Protocol) sia con gli indirizzi IP statici. Belkin consiglia di avere un indirizzo IP riservato per il server console e di farlo rimanere statico quando il server è collegato alla rete.

Interfaccia browser web

L'Interfaccia browser web permette di configurare il server console in modo semplice. L' amministratore può configurare tutte le funzioni via web.

Impostazioni iniziali

Nella sezione seguente sono riportate delle istruzioni per la configurazione dell'indirizzo IP del server console seriale OmniView.

Fase 1 Identificazione dell'indirizzo IP

Dopo aver collegato il server console alla rete e dopo averlo avviato, un server DHCP (Dynamic Host Configuration Protocol) sulla rete assegnerà automaticamente al server console un indirizzo IP, un indirizzo gateway e una maschera di sottorete.

Per individuare l'indirizzo IP della vostra rete, utilizzare l'indirizzo MAC situato sul retro del server console. Se non si rileva un server DHCP sulla rete, il server console si avvierà con il seguente indirizzo IP statico: 192.168.2.156.

Se si desidera collegare vari server console alla stessa rete e non ci sono server DHCP disponibili, collegare un server per volta e modificare l'indirizzo IP statico di ogni unità prima di collegare l'unità successiva.

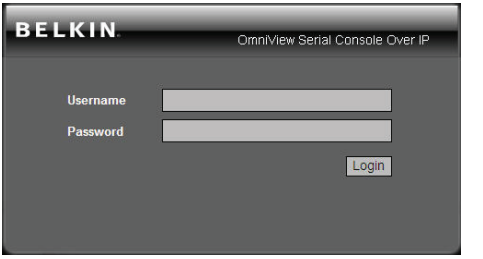
Nota bene: se successivamente si rileva un server DHCP disponibile all'interno della rete, il server console riceverà un nuovo indirizzo IP dal server DHCP. Per mantenere l'indirizzo IP statico originario, occorre disattivare il DHCP (vedi pagina 18).

Fase 2 Accesso all'interfaccia web

Dopo aver individuato l'indirizzo IP del proprio dispositivo, aprire il browser web. A pagina 3 si trova un elenco di tutti i browser supportati.

Digitare l'indirizzo IP del server console nel rispettivo campo del browser, come segue: http://XXX.XXX.XXX.XXX (Ad esempio: http://76.255.43.173). Appare una pagina di login (vedi pagina successiva). Salvare la pagina in Preferiti per una facile consultazione.

Nota bene: HTTPS è utilizzato per le comunicazioni tramite il meccanismo cifrato del protocollo SSL (Secure Socket Layer). Quando ci si collega per la prima volta alla pagina di configurazione HTTPS del server console, potrebbero apparire due messaggi di avviso riguardo la protezione del browser. Fare clic su "Yes" su entrambi i messaggi.



Pagina di login

Digitare il nome utente e la password predefiniti riportati qui di seguito (rispetta maiuscole/minuscole):

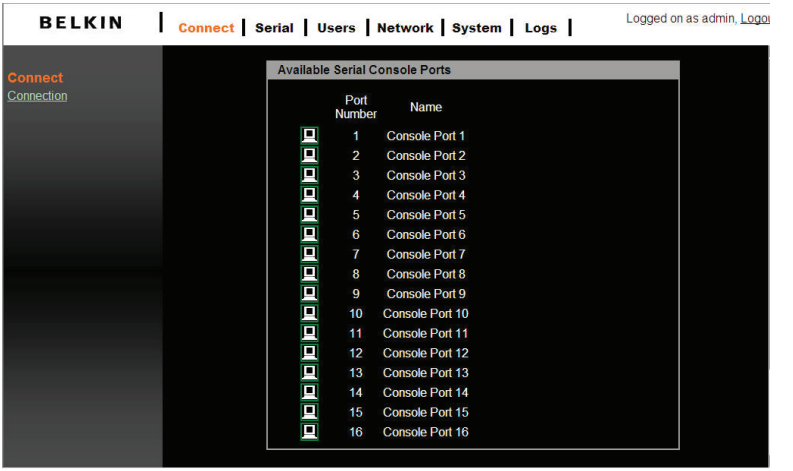
Nome utente	Password
admin	admin

Vi sono due tipi di privilegi di accesso:

Nome utente	Password predefinita	Privilegi di accesso
admin	admin	Accesso completo
(definito dall'utente)	(definito dall'utente)	Può accedere solamente alla “Serial Port” (porta seriale) e “System Status” (stato del sistema)

L'amministratore può aggiungere o eliminare un utente semplicemente dalle pagine web del sistema di amministrazione.

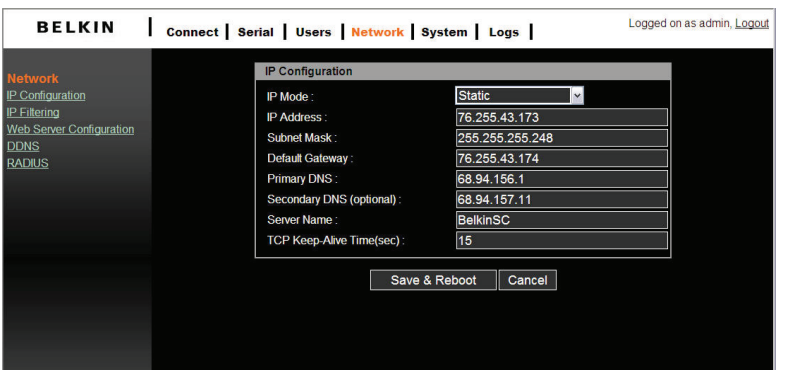
Fare clic su Login . L'interfaccia web si aprirà nella pagina “Connect” (vedi sotto).



Pagina principale "Connect"

Fase 3 Configurazione di rete

Fare clic su “Network” (Rete) per aprire la pagina di configurazione di rete (vedi sotto).



Pagina per la configurazione di rete

Da qui si può assegnare un indirizzo IP statico e cambiare altre impostazioni di rete.

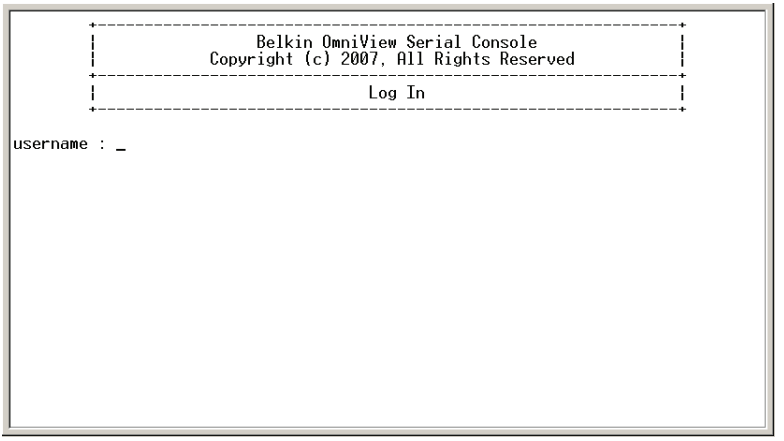
Fare clic su “Save & Reboot” (Salva e riavvia) per memorizzare tutte le impostazioni della configurazione di rete.

Nota bene: se l'utente non usa il browser web per più di **30 minuti,** la sessione di connessione scade e termina.

Assegnazione di un indirizzo IP dalla porta della console VT-100 (Console, Telnet, SSH)

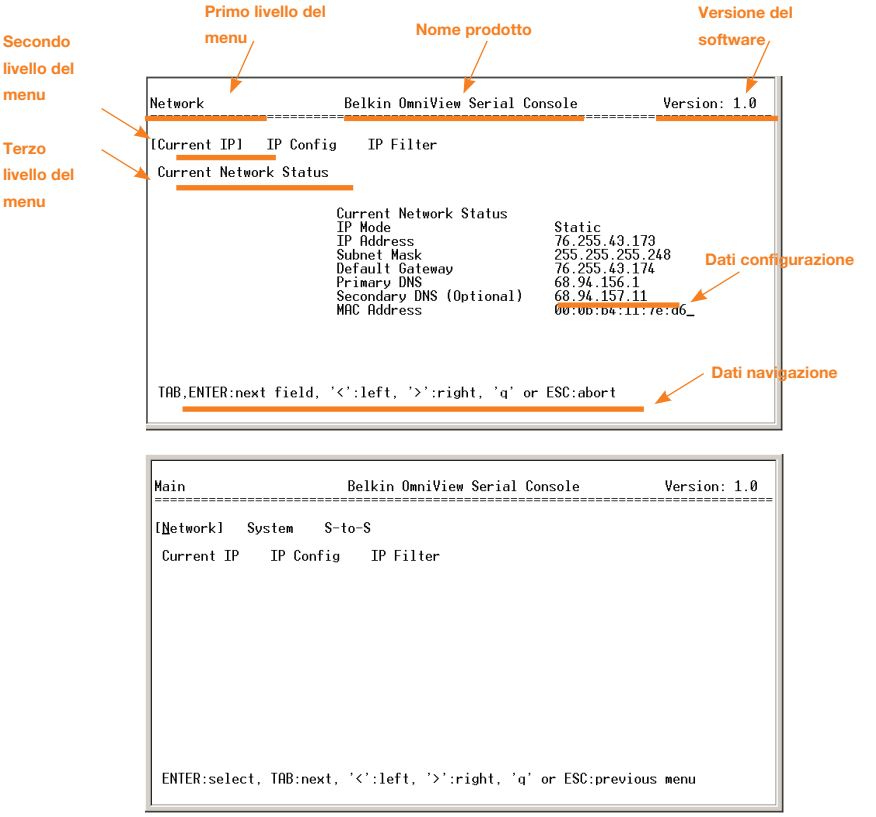
Il server console è inoltre dotato di un'interfaccia a linea di comando con menu di facile utilizzo. Si può semplicemente collegare un terminale VT100 alla porta della console locale per accedere al server console. È utile quando non si conoscono le impostazioni di rete del server console e non si riesce ad accedervi. Mediante la porta della console locale è possibile visualizzare o cambiare le impostazioni (indirizzo IP, maschera di sottorete ecc.).

1. Usando il cavo CAT5 e l'adattatore per la porta della console locale RJ45/DB9F, forniti con il server console Belkin, collegare la porta della console sul pannello posteriore ad una porta seriale su un PC host.
2. Configurare un programma di emulazione terminale, come ad esempio HyperTerminal, usando i seguenti parametri:
   - Baud rate (Trasmissione in baud) = 115200
   - Data bits (Bit di dati) = 8
   - Stop bits (Bit di arresto) = 1
   - Parity (Parità) = none (nessuna)
   - Flow control (Controllo di flusso) = none (nessuno)



Nota bene: i nomi utenti e le password sono uguali a quelli impostati mediante l'interfaccia web. L'impostazione predefinita è “admin/admin”.

La figura di seguito rappresenta la struttura dell'interfaccia.


Primo livello del menu
Nome prodotto
Versione del software
Secondo livello del menu
Terzo livello del menu
Dati configurazione
Dati navigazione
Network Belkin OmniView Serial Console Version: 1.0
[Current IP] IP Config IP Filter
Current Network Status
Current Network Status
IP Mode Static
IP Address 76.255.43.173
Subnet Mask 255.255.255.248
Default Gateway 76.255.43.174
Primary DNS 68.94.156.1
Secondary DNS (Optional) 68.94.157.11
MAC Address 00:0b:b4:11:7e:d6
TAB,ENTER:next field, '<':left, '>':right, 'q' or ESC:abort
Main Belkin OmniView Serial Console Version: 1.0
[Network] System S-to-S
Current IP IP Config IP Filter
ENTER:select, TAB:next, '<':left, '>':right, 'q' or ESC:previous menu

Layout del menu

Network (Rete) > Config IP

La pagina riportata a sinistra raffigura le voci della configurazione IP.

1. Per la **modalità IP** — premere la BARRA SPAZIATRICE per selezionare la modalità statica o DHCP.
2. Per **l'indirizzo IP, la maschera di sottorete, il default gateway, il DNS primario e secondario** — È possibile cambiare queste impostazioni di rete.
3. Dopo aver cambiato le impostazioni ed aver premuto il tasto "Invio" per l'ultima volta, il server console richiede di confermare con "YES" o "NO". Se si sceglie "YES" (Sì), il server console si riavvia e vengono salvate le impostazioni nella scheda di memoria.

Network (Rete) > Current IP (IP attuale)

Per visualizzare le impostazioni di rete attuali.

Network (Rete) > IP Filter (Filtraggio IP)

Per attivare/disattivare il filtraggio IP.

System (Sistema) > Reboot (Riavvia)

Per riavviare il server console.

System > Reset to Default (Ripristina i valori predefiniti)

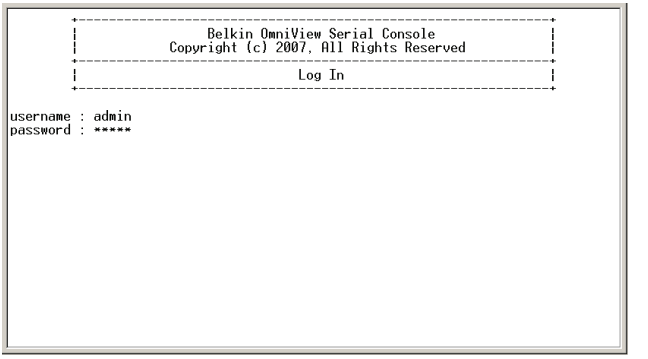
Per ripristinare le impostazioni predefinite.
Nota bene: solo l'**amministratore** può effettuare questa operazione.

System > Status (Stato del sistema)

Per visualizzare lo stato del sistema.

S-to-S > Select Serial-to-Serial Port (Seleziona porta seriale/seriale)

Per attivare la connessione da porta seriale a porta seriale dalla porta 16. Per ulteriori informazioni consultare la sessione "Modalità da seriale a seriale" a pagina 34.



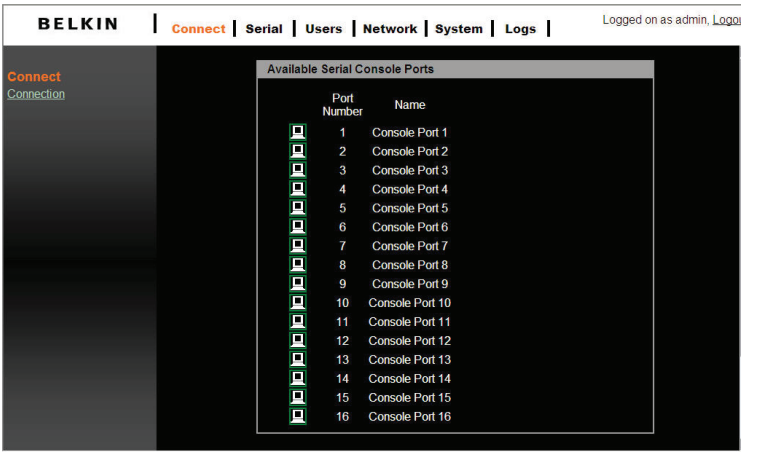
Nota bene:
solo l'**amministratore** può collegarsi alla VT-100. Gli altri utenti non sono autorizzati a configurare con la VT-100.

Interfaccia di gestione basata sul web

Il server console è compatibile sia con i protocolli HTTP sia HTTPS (HTTP over SSL). Gli utenti devono autenticarsi collegandosi al sistema e digitando il nome utente e la password corretti.

Per accedere alle pagine per la gestione web del server console, digitare l'indirizzo IP o il nome host risolvibile nella barra degli indirizzi. In questo modo apparirà automaticamente la pagina di login.

La figura alla pagina seguente indica la homepage di un'interfaccia per la gestione web. Nella parte superiore della pagina appare la barra dei menu. A sinistra della pagina appare il sottomenu, che permette di modificare i parametri delle impostazioni della voce selezionata nel menu principale.

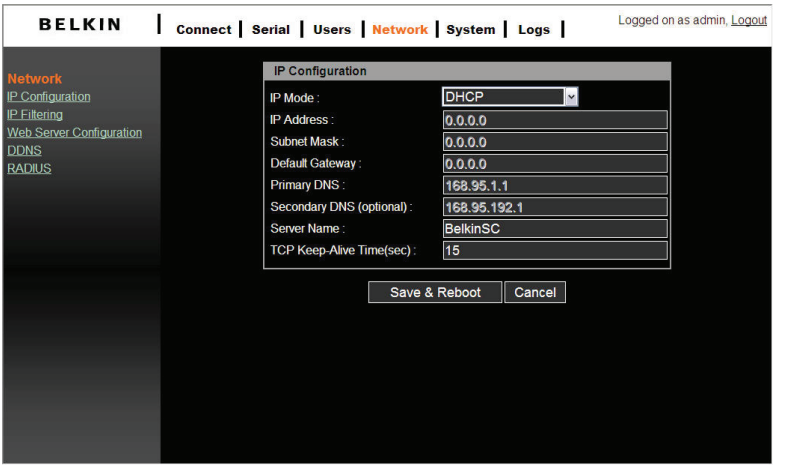


Laddove possibile, la pagina permette agli utenti di applicare o eliminare le proprie azioni. Per applicare le modifiche, selezionare "Apply" (applica) e i nuovi valori saranno applicati alla configurazione. Qualora non si volessero salvare i nuovi valori, è sufficiente fare clic su "Cancel" (Annulla) e tutte le modifiche apportate saranno eliminate e saranno ripristinati i valori precedenti.

È possibile configurare le impostazioni IP di rete mediante la VT-100 o l'interfaccia web. Questa sessione descrive il procedimento di configurazione mediante l'interfaccia web.

Configurazione IP

Il server console richiede un indirizzo IP valido per poter funzionare all'interno dell'ambiente di rete dell'utente. Se l'indirizzo IP non è disponibile al momento, contattare l'amministratore di sistema per avere un indirizzo IP valido per il server console.



È possibile scegliere tra due diverse assegnazioni IP:

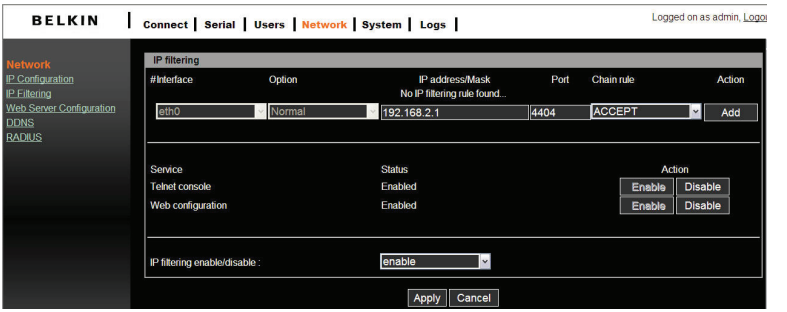
- IP statico
- DHCP (Protocollo di Configurazione Host Dinamica)

L'unità viene fornita con il protocollo DHCP impostato come predefinito. Se non si rileva un server DHCP sulla rete, il server console si avvierà con il seguente indirizzo IP statico: 192.168.2.156.

Le nuove impostazioni relative all'indirizzo IP vengono salvate facendo clic su “Save & Reboot” (salva e riavvia).

Filtraggio IP

La funzione di filtraggio IP impedisce ad utenti non autorizzati di accedere al server console mediante delle regole.



L'indirizzo/maschera IP specifica il range dell'host digitando l'indirizzo IP di base seguito da "/" e dalla maschera di sottorete ("/" è necessario per separare l'indirizzo IP dalla maschera di sottorete). Gli indirizzi IP degli host vengono filtrati in base alla regola configurata.

La tabella sotto riportata mostra degli esempi di impostazioni di indirizzi/maschera IP.

Range dell'host specificato	Indirizzo IP dell'host di base	Maschera di sottorete
Qualsiasi host	0.0.0.0	0.0.0.0
192.168.2.120	192.168.2.120	255.255.255.255
192.168.2.1 ~ 192.168.2.254	192.168.2.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.2.1 ~ 192.168.1.126	192.168.2.0	255.255.255.128

La "Port" è una porta o il range della porta del server console ai quali gli host provano a collegarsi.

Catena di regole

La catena di regole determina se permettere l'accesso agli host o meno. Può avere uno o due valori:

- **ACCEPT (ACCETTA):** accesso consentito
- **DROP (RILASCIA):** accesso non consentito

Quando il server console riceve un pacchetto TCP, lo processa applicando la catena di regole come illustrato di seguito. L' ordine del procedimento è importante: il pacchetto entrerà prima di tutto nella catena di regole 1. Se possiede le caratteristiche specificate dalla regola, viene selezionato, altrimenti passerà alla regola 2.

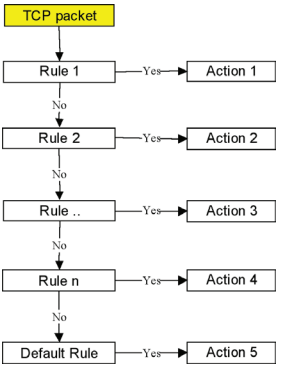
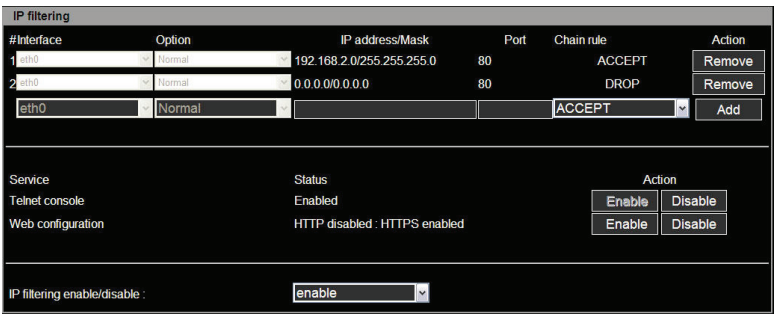


Fig. 4 Catena di regole del filtraggio IP

Si può aggiungere una nuova regola al filtraggio IP impostando le proprietà nella prossima riga disponibile. Una volta impostata la regola, fare clic su "Add" (Aggiungi) per salvare l'operazione. Per eliminare una regola, fare clic su “Remove” (Elimina).



Nell'esempio sopra riportato, le regole sono applicate nel seguente ordine:

#1. Gli host che appartengono alla sottorete 192.168.2.x hanno l'accesso garantito al server console (attraverso la porta http 80).

#2. L'accesso al server console (attraverso la porta http 80) non è garantito a nessun host.

Una volta applicate le regole, solo gli host che appartengono alla sottorete 192.168.2.x possono accedere al server console (mediante la porta http 80).

Oltre alla catena di regole del filtraggio IP menzionato precedentemente, l'interfaccia web offre un modo comodo per attivare/disattivare la porta telnet (porta 23) o la porta di configurazione web (porta 80/443). Questi servizi sono particolarmente indicati per la modalità di configurazione Console-Server. Facendo clic su “Enable/Disable” (Attiva/disattiva) nel campo “Action” (Azione) si può modificare/aggiungere una catena di regole velocemente e senza dover modificare manualmente la regola.

Nota bene:
per poter ottenere un migliore allineamento di testo, è consigliabile effettuare l'allineamento con un client compatibile con telnet VT-100. PuTTY è uno dei client telnet consigliati tra coloro che offrono un allineamento di testo dell'interfaccia utente e può essere scaricato da

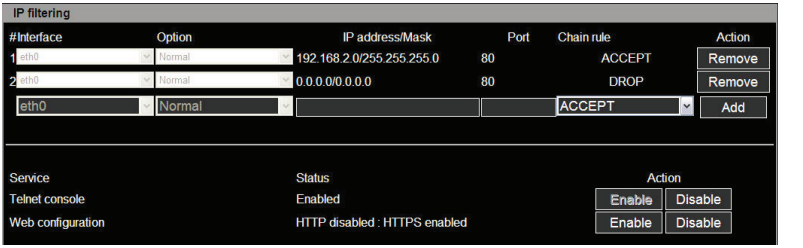
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Configurazione del server web

Il server web del server console è compatibile contemporaneamente sia con i protocolli HTTP sia HTTPS (HTTP over SSL).
Si può selezionare il metodo per l'autenticazione utente dell'accesso via web. Il server console attualmente offre i metodi di autenticazione locale e RADIUS.

Locale

Per impostazione predefinita il server console si dirige verso il database locale per l'autenticazione dell'utente via server web.



RADIUS e locale

Per l'autenticazione di un account utente il server console si dirige innanzitutto al server RADIUS. Se non si trova l'account utente o il server RADIUS non è disponibile, il server console effettua una ricerca tra i propri database locali per trovare l'account utente. Se non si trovano né un database RADIUS né locale, l'unità non consente l'accesso all'utente. Il server RADIUS può essere configurato dalla pagina di configurazione "RADIUS server". Leggere pagina 24.

DNS dinamico

Se un utente collega il server console ad una linea DSL oppure usa una configurazione DHCP per ottenere un indirizzo IP dinamico dalla rete, l'indirizzo IP potrebbe cambiare. In questo caso potrebbe essere difficile sapere se l'indirizzo IP sia cambiato o quale sia il nuovo indirizzo IP.

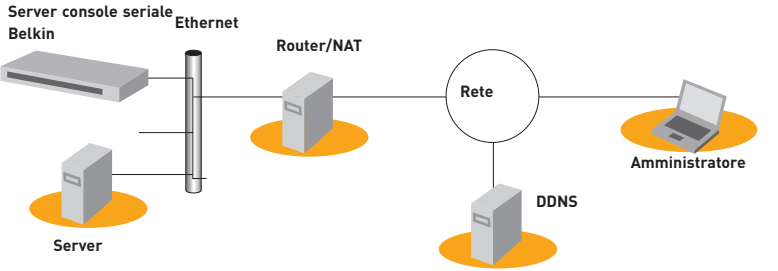
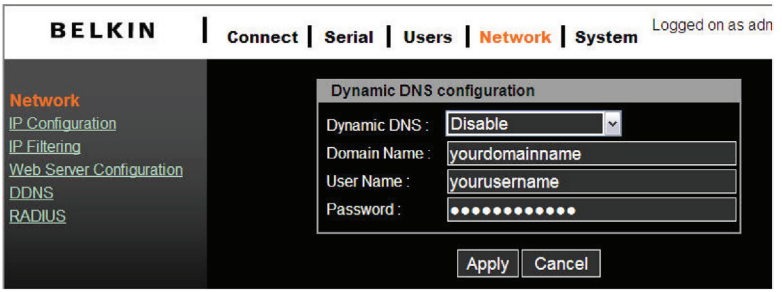


Fig. 5 DNS dinamico

Il servizio di DNS dinamico è offerto da vari provider Internet ed organizzazioni in modo tale da poter ovviare al problema sopra riportato. Usando un servizio di DNS dinamico si può accedere al server console mediante il nome host registrato nel server DNS dinamico, indipendentemente da eventuali cambi dell' indirizzo IP. Per impostazione predefinita il server console supporta solamente il servizio di DNS dinamico della Dynamic DNS Network Services, LLC (www.dyndns.org).

Per usare il DNS dinamico offerto dalla Dynamic DNS Network Services bisogna aprire un account nel centro informazioni di rete NIC (Network Information Center - http://members.dyndns.org) riservato ai membri. Dopo essersi collegati al loro "Dynamic DNS Network Services Members NIC" è possibile aggiungere un nuovo collegamento host DNS dinamico.

Dopo aver attivato il DNS dinamico nel menu di configurazione "Dynamic DNS", bisogna digitare il nome di dominio registrato, il nome utente e la password. Dopo aver applicato le modifiche, sarà possibile accedere al server console semplicemente usando il nome di dominio. Il DNS (Domain Name Systems) è il servizio Internet che traduce i nomi di domini in indirizzi IP.



Nota bene:
Il campo "domain-name" (Nome di dominio) richiede un Qualified Domain Name (FQDN), anziché un semplice nome host registrato.

RADIUS

L'autenticazione è il procedimento per identificare un individuo e generalmente si basa su un nome utente ed una password. Il server console supporta varie opzioni di autenticazione, come ad esempio “Local” (locale) e “RADIUS” per autenticare gli utenti che accedono alla porta seriale. Quando l'autenticazione è impostata su "Local", l'unità usa solamente il proprio elenco di utenti per autenticarne uno. Qualora fosse stato configurato diversamente, il server console richiederà un'autenticazione da server di autenticazione esterni (ad esempio, RADIUS). La figura di seguito mostra il concetto del processo di autenticazione degli utenti quando si usa un server di autenticazione esterno.

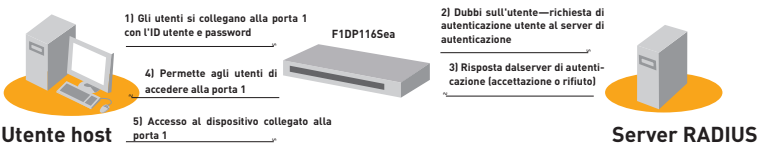
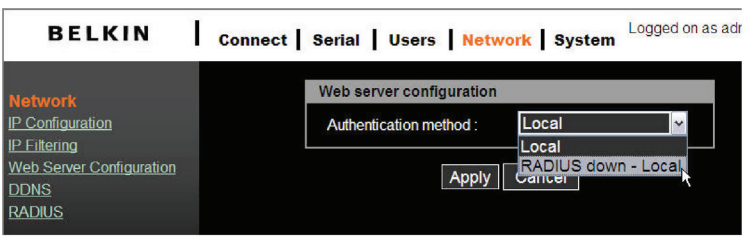
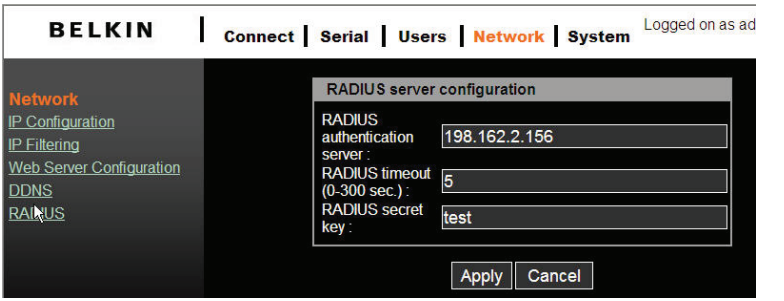

1) Gli utenti si collegano alla porta 1 con l'ID utente e password
F1DP116Sea
2) Dubbi sull'utente—richiesta di autenticazione utente al server di autenticazione
3) Risposta dalserver di autenti-cazione (accettazione o rifiuto)
4) Permette agli utenti di accedere alla porta 1
5) Accesso al dispositivo collegato alla porta 1
Utente host
Server RADIUS

Fig. 6 RADIUS



Configurazione del server RADIUS



Nota bene:
per poter rendere il servizio RADIUS efficace, bisogna installare un server RADIUS prima

HTTPS/SSL

Il server console è compatibile contemporaneamente sia con i protocolli HTTP sia HTTPS (HTTP over SSL). È possibile attivare o disattivare la funzione di protezione di ogni porta singolarmente.

Il protocollo HTTPS offre una interfaccia protetta e crittografata mediante SSL (secure sockets layer).

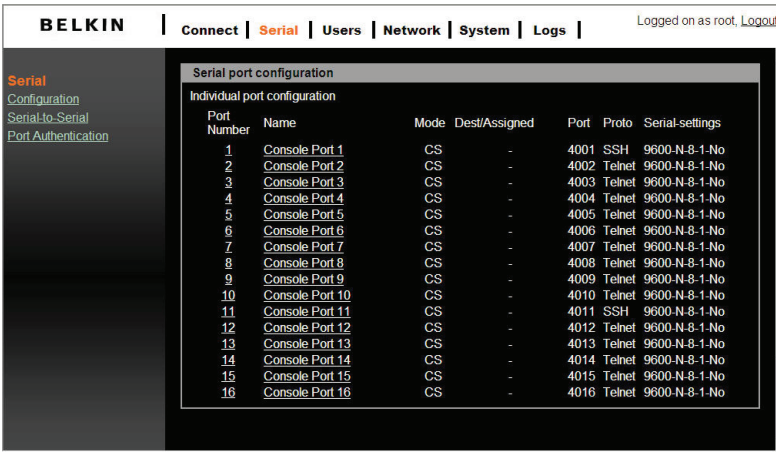
Seguire le seguenti fasi per il protocollo HTTPS:

1. Cambiare la URL da “http://xxx.xxx.xxx/” a “https://xxx.xxx.xxx/”.
2. Dopo aver stabilito la connessione, il browser visualizzerà l'icona “Lock” (Lucchetto).

Fare doppio clic sul simbolo del lucchetto per visualizzare le informazioni relative al certificato.

Configurazione

Dal menu "Serial" fare clic su "Configuration" (Configurazione) per visualizzare l'elenco delle porte.

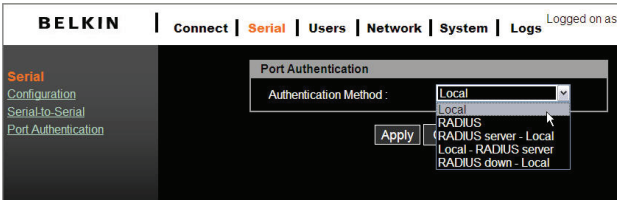

BELKIN
Connect | Serial | Users | Network | System | Logs |
Logged on as root, Logout
Serial
Configuration
Serial-to-Serial
Port Authentication
Serial port configuration
Individual port configuration
Port Number | Name | Mode | Dest/Assigned | Port | Proto | Serial-settings
1 Console Port 1 CS - 4001 SSH 9600-N-8-1-No
2 Console Port 2 CS - 4002 Telnet 9600-N-8-1-No
3 Console Port 3 CS - 4003 Telnet 9600-N-8-1-No
4 Console Port 4 CS - 4004 Telnet 9600-N-8-1-No
5 Console Port 5 CS - 4005 Telnet 9600-N-8-1-No
6 Console Port 6 CS - 4006 Telnet 9600-N-8-1-No
7 Console Port 7 CS - 4007 Telnet 9600-N-8-1-No
8 Console Port 8 CS - 4008 Telnet 9600-N-8-1-No
9 Console Port 9 CS - 4009 Telnet 9600-N-8-1-No
10 Console Port 10 CS - 4010 Telnet 9600-N-8-1-No
11 Console Port 11 CS - 4011 SSH 9600-N-8-1-No
12 Console Port 12 CS - 4012 Telnet 9600-N-8-1-No
13 Console Port 13 CS - 4013 Telnet 9600-N-8-1-No
14 Console Port 14 CS - 4014 Telnet 9600-N-8-1-No
15 Console Port 15 CS - 4015 Telnet 9600-N-8-1-No
16 Console Port 16 CS - 4016 Telnet 9600-N-8-1-No

Da notare che se la "Serial port" (Porta seriale) è disattivata, i caratteri del pannello “Serial port configuration” (Configurazione della porta seriale) saranno grigio scuro. Una porta seriale attivata sarà invece rappresentata in grassetto bianco.

Autenticazione della porta

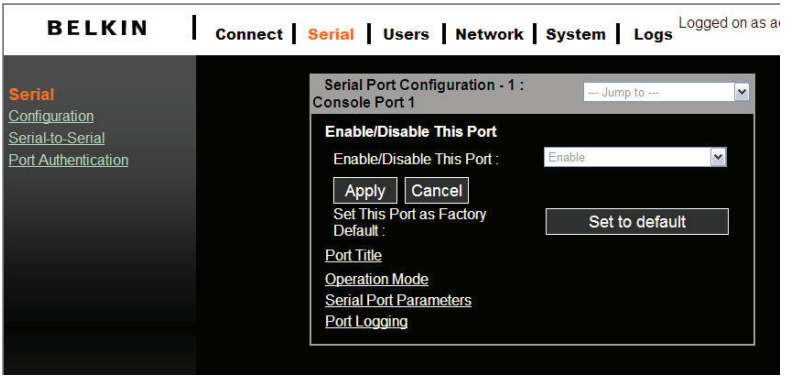
L'autenticazione è il procedimento per identificare un individuo e generalmente si basa su un nome utente ed una password. Il server console supporta varie opzioni di autenticazione, come ad esempio “Local” (locale) e “RADIUS” per autenticare gli utenti che accedono alla porta seriale. Leggere pagina 23.

Quando l'autenticazione è impostata su "Local", l'unità usa solamente il proprio elenco di utenti per autenticare un utente. Qualora fosse configurato su RADIUS, il server console richiederà un'autenticazione da server di autenticazione esterni (ossia RADIUS). La figura di seguito mostra il concetto del processo di autenticazione degli utenti quando si usa un server di autenticazione esterno.



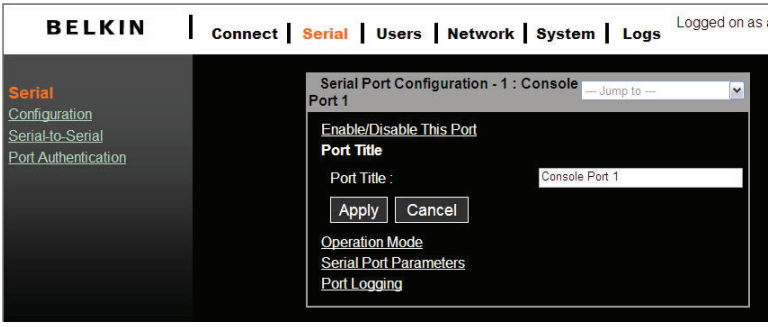
Abilitazione / Disabilitazione porta

Ogni porta seriale può essere abilitata o disabilitata separatamente. Un utente non può accedere ad una porta seriale disabilitata. Gli utenti possono resettare le impostazioni predefinite della porta seriale facendo clic sul pulsante “Set to default” (Imposta valori predefiniti).



Titolo della porta

Gli utenti posso aggiungere delle informazioni per descrivere ciascuna porta a seconda del dispositivo al quale sono collegate.



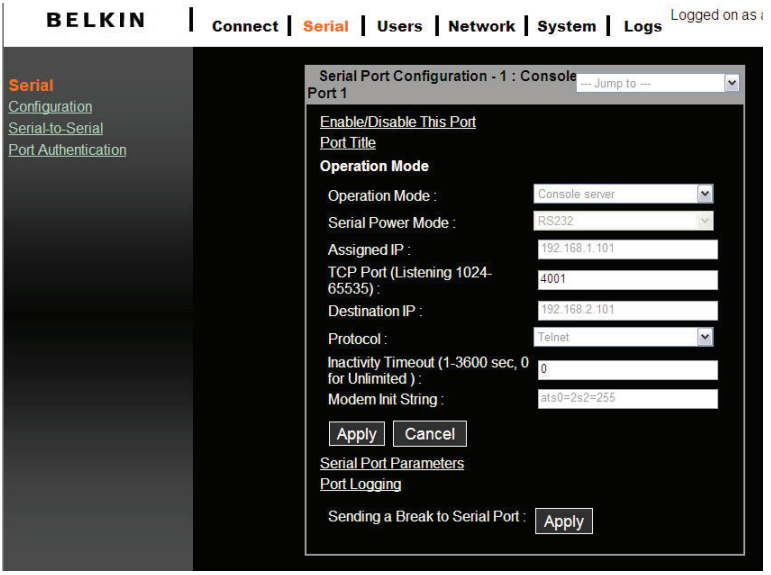
Per selezionare e configurare un'altra porta si può usare la scorciatoia “--Jump to--”, situata nell'angolo in alto a destra.

Modalità di funzionamento

Il server console è provvisto di quattro modalità di funzionamento, descritte di seguito.

Nota bene:

- Nella modalità da seriale a seriale, l'ultima porta (es. porta 16) può essere utilizzata come “External ESP (Entry Serial Port)” (Porta di entrata seriale esterna). Per ulteriori informazioni, consultare la sezione "Modalità da seriale a seriale".



Modalità "Console-Server"

Se si configura una porta seriale come server console si crea una presa TCP sull'unità che ascolta una connessione telnet o SSH client. Quando ci si collega ad una presa TCP si accede al dispositivo collegato alla porta seriale, come se il dispositivo fosse collegato direttamente alla rete. I flussi di dati possono essere spediti avanti e indietro tra il dispositivo e il programma telnet/SSH client. Inoltre quando è attiva la modalità "console-server" è supportato anche il protocollo RawTCP.

Quando è in modalità "console-server" è possibile configurare i seguenti parametri::

Ascolto del numero di porta TCP
Inoltre è possibile accedere ad una porta seriale mediante l'indirizzo IP del server console ed ascoltare il numero della porta TCP della porta seriale.

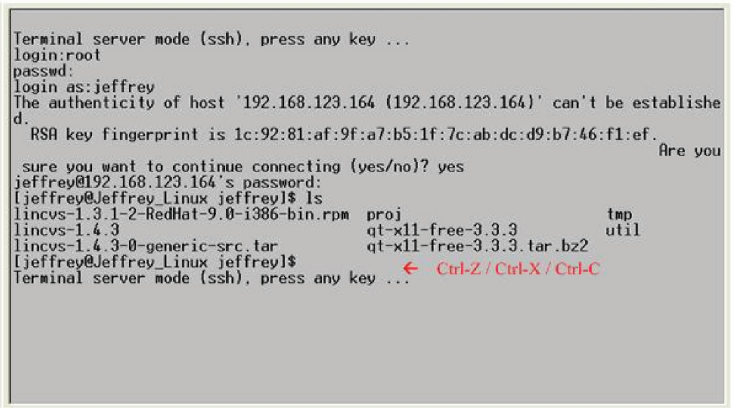
Se l'indirizzo IP del server console e la porta seriale assegnati sono 192.168.123.100 e il numero della porta TCP è 4001, l'utente può collegarsi alla porta nel seguente modo: telnet 192.168.123.100 4001

Protocollo
Come protocollo selezionare “Telnet”, “SSH”, o “Raw TCP”. Qualora gli utenti usassero un programma client telnet, selezionare "Telnet". Qualora gli utenti usassero un programma client SSH, selezionare "SSH". Quando si seleziona “Raw TCP” la comunicazione TCP socket diretta è disponibile tra il server console e l'host remoto.

Intervallo di inattività
Attivare questa funzione per evitare che un client mantenga una connessione TCP quando non vi sia attività su una porta seriale per un periodo di tempo lungo. Se “Inactivity timeout” (Intervallo di inattività) è attivato e se non vi è stato scambio di dati tra il server console e il client telnet/SSH per un periodo di tempo prestabilito nell'intervallo di inattività (ovvero se non vi è stata attività attraverso la porta seriale) la sessione TCP corrente verrà interrotta automaticamente. Se si vuole mantenere la connessione attiva a tempo indeterminato, impostare il periodo di inattività su "0".

Connessione TCP Keep-Alive (Non è richiesta alcuna configurazione)
Per impedire che la connessione TCP si arresti,il server console continua a verificare lo stato della connessione tra il client telnet/SSH e il server console inviando regolarmente dei pacchetti “keep alive”. Se il client telnet/SSH non risponde ai pacchetti, il sistema deduce che la connessione è stata interrotta. Il server console interromperà allora la connessione telnet/SSH corrente, indipendentemente dalle impostazioni di inattività. Così si fa in modo che la connessione TCP non si arresti quando un'applicazione viene chiusa in modo non corretto oppure quando si interrompe il collegamento di rete.

Modalità terminal server
Quando è attiva la modalità "terminal server", la porta seriale del server console è configurata in modo tale da aspettare i dati dal dispositivo collegato alla porta. Se i dati vengono rilevati, il server console inizia la sessione TCP come client telnet o SSH ad un server predefinito. Prima che la porta possa essere configurata per un client telnet o SSH, il server deve essere definito dagli utenti. Questa modalità può essere utilizzata per accedere a server collegati in rete da un terminale seriale. Inoltre quando la modalità terminal server è attiva è supportato anche il protocollo RawTCP.



Per terminare una sessione telnet/SSH/RawTCP in modalità terminal server, si possono usare delle sequenze di tasti di scelta rapida (Ctrl-Z / Ctrl-X / Ctrl-C).

Modalità modem dial-in

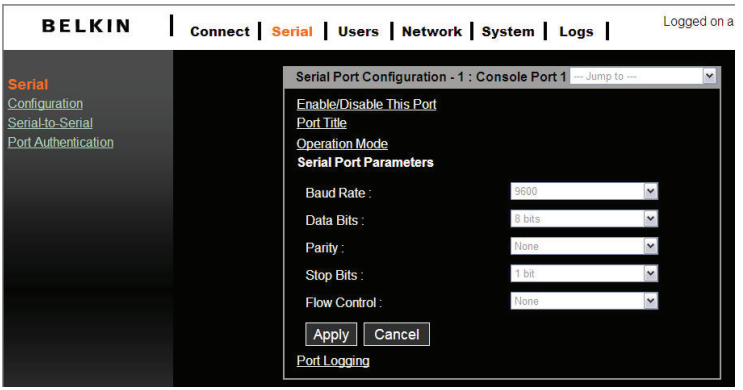
Quando è in questa modalità, il server console pensa che un modem esterno sia collegato alla porta seriale ed aspetta una connessione dial-in da una sede remota. Quando un utente chiama usando un'applicazione terminale, il server console accetta la connessione e visualizza il messaggio di avviso o il menu per l'utente collegato.

Modalità da seriale a seriale

Per ulteriori informazioni sulla modalità da seriale a seriale, consultare la sezione "Modalità da seriale a seriale" a pagina 34.

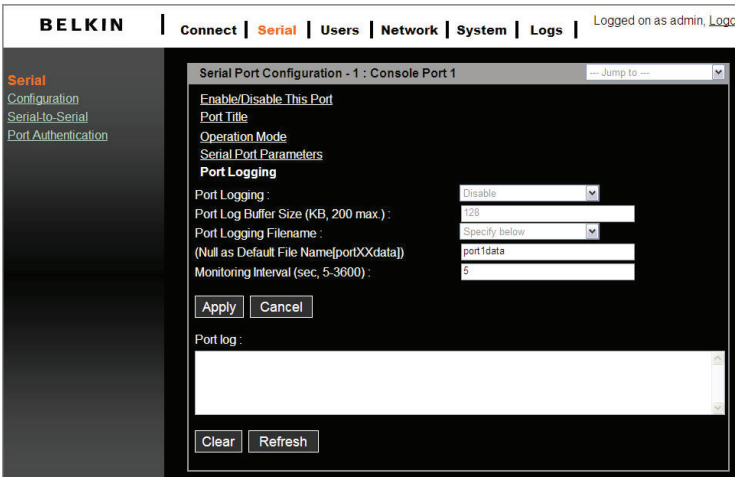
Parametri della porta seriale

Per collegare il dispositivo seriale alla porta seriale del server console, i parametri della porta seriale del server console devono corrispondere esattamente ai requisiti del dispositivo seriale collegato.



Registrazione della porta

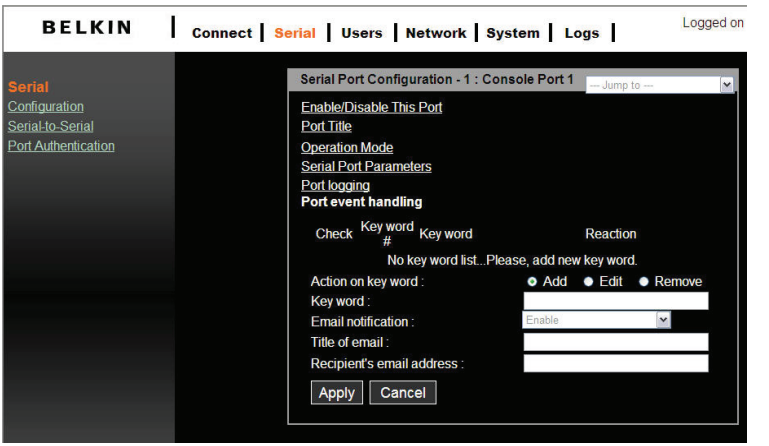
Quando è in modalità console-server, i dati ricevuti dalla porta seriale rilevata verranno salvati nella memoria dell'unità.



La funzione “Port logging” (registrazione della porta) è valida e visibile solo se la modalità di funzionamento della porta seriale è impostata sulla modalità console-server.

Se l'opzione “Port logging” è spuntata, l'utente può chiedere al server console di trovare una parola chiave prestabilita dai dati di registrazione porta ed inviare un'e-mail all'amministratore dalle configurazioni “Port event handling”. Ogni risposta può essere configurata individualmente in base ad ogni parola chiave. Le risposte possono essere inviate per e-mail.

Fare clic su “Port event handling”.



Il buffer di memoria per la registrazione dei dati è di 192 K per porta. Se la registrazione dei dati supera la capacità della memoria, i nuovi dati sovrascriveranno i vecchi dati.

Funzione break

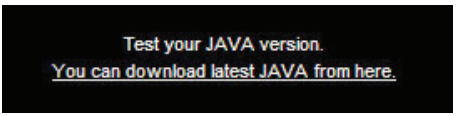
Quando è in modalità "console-server", il server console può inviare un segnale "break" al dispositivo seriale collegato. Un break a volte è utilizzato per effettuare il reset di una linea di comunicazione o per cambiare la modalità operativa dell'hardware di comunicazione, come ad esempio un MODEM. Alcuni dispositivi di destinazione, come ad esempio il server Sun™ Solaris™ , per generare un messaggio "OK" richiedono un carattere nullo (break) . L'effetto di “Sending a break through serial port” (Invio di un break mediante una porta seriale) è come premere "STOP-A" su una tastiera Sun. Per poter inviare un break ad un dispositivo seriale, configurare quest'ultimo in modalità "Console Server" ed usare “Telnet” o “RawTCP” come protocollo. Fare clic su "Apply" (Applica) per inviare il segnale di break alla porta seriale desiderata e quindi al computer o al server collegato.

Connessione

Il server console fornisce un accesso basato sul web al dispositivo seriale di destinazione senza aver bisogno di un programma per client telnet separato. Ciò avviene grazie ad una applet Java.

Una applet Java è usata per offrire un'interfaccia utente testuale per accedere alla porta seriale. Questa applet Java supporta solamente la modalità telnet quando è in modalità "console-server". L'utente non può accedere alla porta seriale via web quando la modalità host della porta è impostata su una connessione RawTCP. Per poter accedere alla porta, viene richiesto di digitare l'ID utente e la password. Una volta autenticato, l'utente può accedere alla porta seriale.

Per verificare la compatibilità con Java, usare l'hyperlink situato nella parte inferiore della pagina "Connect" oppure usare il link di seguito riportato per scaricare la versione di Java più recente.



Assicurarsi di aver abilitato l'opzione di supporto Java del browser e controllare la versione di Java Runtime Environment (conosciuta come versione JRE). Qualora si volesse anche il servizio HTTP sicuro (HTTPS) è necessaria la versione 1.6.0 o successiva.

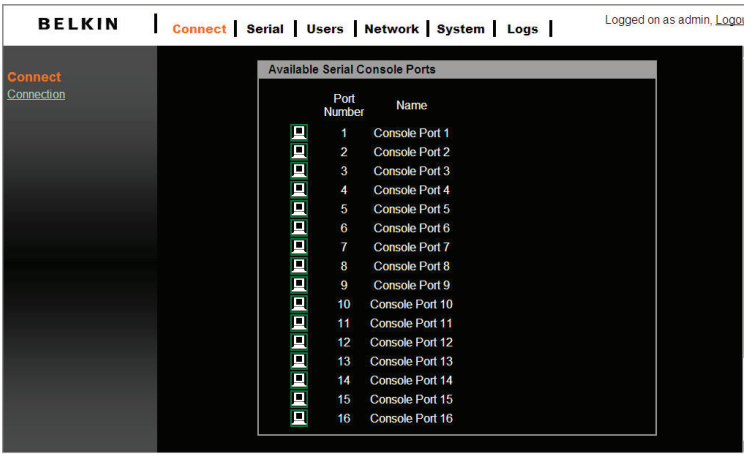
Nota bene:

- Per poter avviare questa funzione, è necessario avere installato nel sistema JRE versione 6.0 o successive. È possibile scaricare il software Java più recente dal sito:http://www.java.com/en/download/.

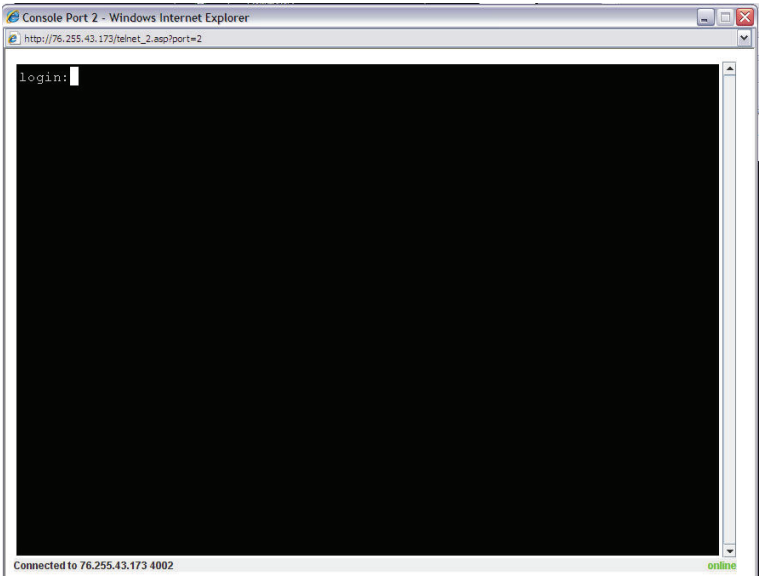
Telnet Java Applet

1. Selezionare il protocollo telnet da “Serial > Configuration > Operation mode” (Seriale > Configurazione > Modalità di funzionamento).

Dal menu in alto selezionare “Connect” e fare clic sull'icona del terminale a sinistra. Si apre una nuova finestra con l'applicazione dell'emulazione del terminale che richiede di connettersi. Se la finestra è vuota, verificare la compatibilità del sistema con la versione di Java.



2. Digitare il nome utente e la password per connettersi, in modo tale da poter utilizzarla come se si avesse un programma client telnet. (e.g., Telnet DOS program, PuTTY).



Nota bene: il nome della porta seriale appare nella barra della finestra. Inoltre verrà visualizzato l'indicatore dello stato della connessione nella parte in basso a destra della finestra.

Modalità da seriale a seriale

La modalità da seriale a seriale permette di usare un semplice dispositivo terminale (monitor e tastiera) per accedere e controllare qualsiasi dispositivo collegato al server console sulle porte da 1 a 15. Si può inoltre utilizzare un convertitore per reti di terminali esterno, come l'F1D084Eea Belkin, per collegare il server console ad uno switch KVM e rafforzarne il controllo.

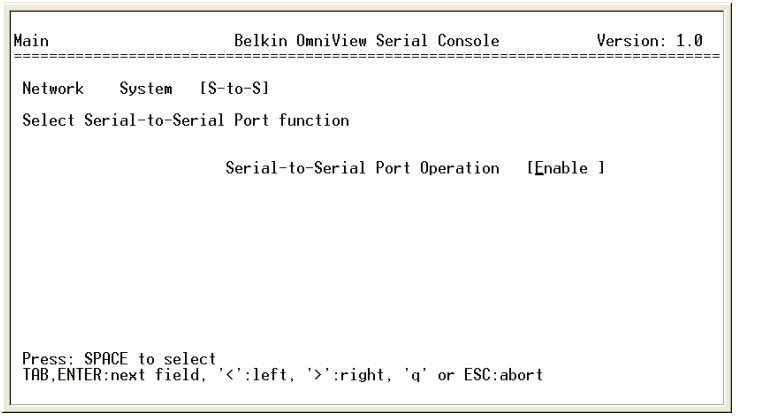
Installazione

Per l'installazione, collegare il dispositivo terminale alla porta 16 del server console. In questo modo si potrà accedere ad un dispositivo seriale collegato alle porte da 1 a 15.

Attivazione e configurazione della modalità da seriale a seriale

Per configurare la modalità da seriale a seriale:

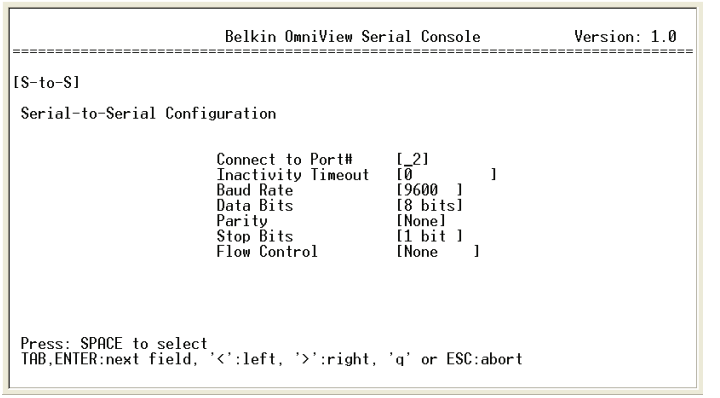
1. Avviare la modalità console VT-100 (consultare la sezione “Assegnazione di un indirizzo IP dalla porta della console VT-100 (Console, Telnet, SSH)” per ulteriori dettagli) per visualizzare la schermata sottostante.
2. Andare al secondo livello del menu [S-to-S] “Serial-to-Serial port operation” e premere la BARRA SPAZIATRICE per selezionare “ENABLE” (Attiva). Confermare la modifica per fare riavviare automaticamente il sistema.

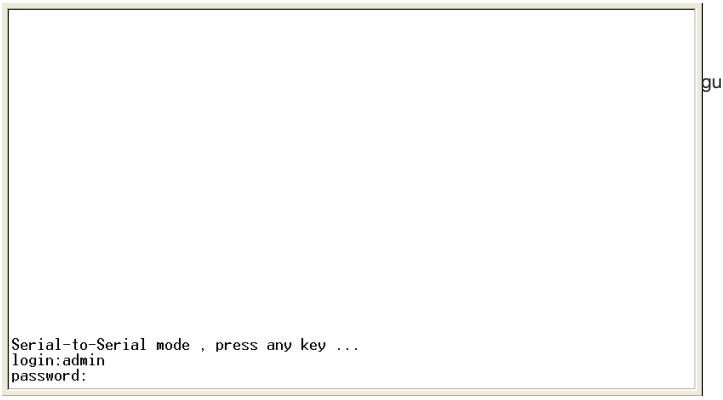

Main Belkin OmniView Serial Console Version: 1.0
Network System [S-to-S]
Select Serial-to-Serial Port function
Serial-to-Serial Port Operation [Enable]
Press: SPACE to select
TAB,ENTER:next field, '<':left, '>':right, 'q' or ESC:abort

3. Quindi disconnettersi dalla console locale ed iniziare una nuova sessione del terminale collegandosi alla porta 16.
4. Dopo il riavvio (richiede circa un minuto) appare la schermata raffigurata nella pagina seguente. Configurare ogni impostazione di configurazione. Inserire il valore per l'“Inactivity timeout” (intervallo di inattività) e premere la BARRA SPAZIATRICE per selezionare le impostazioni relative alle altre voci.

Nota bene:

- per poter visualizzare la schermata di configurazione da seriale a seriale, è necessario abilitare la modalità da seriale a seriale. Per poter garantire la migliore compatibilità con dispositivi monitor terminali di terzi, la trasmissione in baud predefinita è impostata su 9600 8N1 (non riconfigurabile).





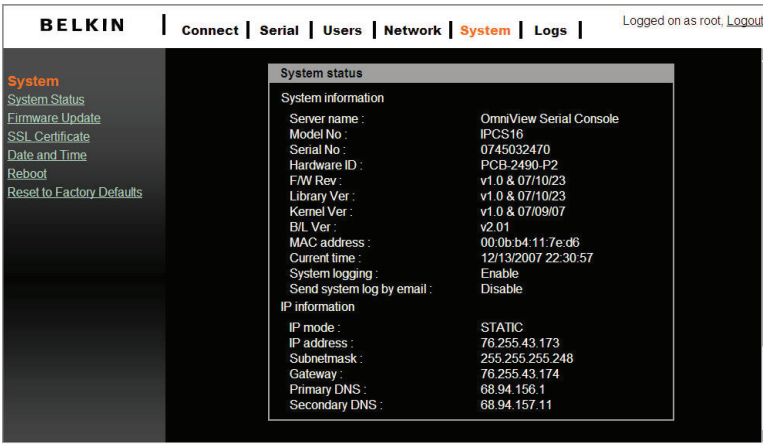
guito.

6. Digitare il nome utente e la password. Si stabilisce la connessione del canale dati tra la porta 16 e la porta seriale selezionata, in modo tale che l'amministratore possa controllare il dispositivo seriale o il server.
7. Premere i tasti “Cntl” e “C” per uscire dalla modalità da seriale a seriale e ritornare alla schermata principale della console.

La pagina web dà delle impostazioni di sola lettura della modalità da seriale a seriale; cambierà automaticamente a seconda della modifica delle impostazioni della console VT-100. Fare clic su "Cancel" (Annulla) per ripristinare i valori.

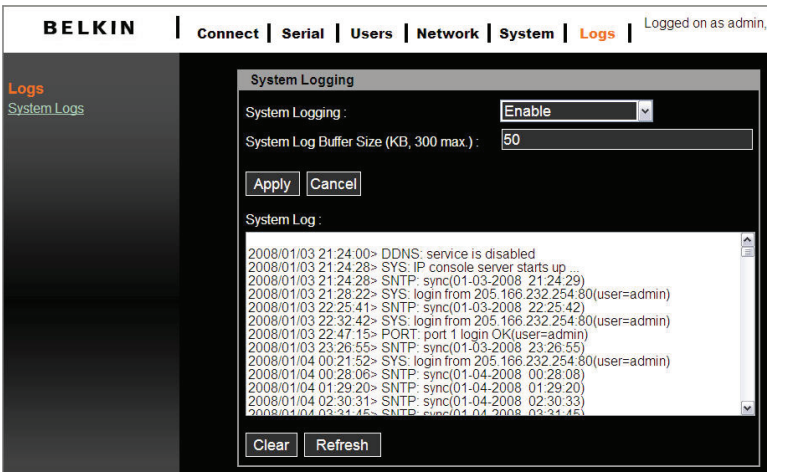
Stato del sistema

La pagina “System Status” (Stato del sistema) raccoglie un elenco con le informazioni di sistema correnti, quali il nome, il numero di serie, la versione del firmware, l'indirizzo Mac, l'ora e le impostazioni di rete. Da questa pagina non è possibile cambiare i dati. Questa pagina si aggiorna automaticamente ogni 10 secondi.



Registrazione del sistema

È possibile attivare o disattivare il procedimento di registrazione del sistema e impostare la capacità buffer della registrazione. Il valore predefinito della capacità buffer della registrazione del sistema è di 50 KB e può arrivare fino ad un massimo di 300 KB. Se la registrazione dei dati supera la capacità preimpostata della memoria, i nuovi dati sovrascriveranno i vecchi dati.


BELKIN
Connect | Serial | Users | Network | System | Logs |
Logged on as admin,
Logs
System Logs
System Logging
System Logging :
Enable
System Log Buffer Size (KB, 300 max.) :
50
Apply
Cancel
System Log :
2008/01/03 21:24:00> DDNS: service is disabled
2008/01/03 21:24:28> SYS: IP console server starts up ...
2008/01/03 21:24:28> SNTP: sync(01-03-2008 21:24:29)
2008/01/03 21:28:22> SYS: login from 205.166.232.254:80(user=admin)
2008/01/03 22:25:41> SNTP: sync(01-03-2008 22:25:42)
2008/01/03 22:32:42> SYS: login from 205.166.232.254:80(user=admin)
2008/01/03 22:47:15> PORT: port 1 login OK(user=admin)
2008/01/03 23:26:55> SNTP: sync(01-03-2008 23:26:55)
2008/01/04 00:21:52> SYS: login from 205.166.232.254:80(user=admin)
2008/01/04 00:28:06> SNTP: sync(01-04-2008 00:28:08)
2008/01/04 01:29:20> SNTP: sync(01-04-2008 01:29:20)
2008/01/04 02:30:31> SNTP: sync(01-04-2008 02:30:33)
Clear
Refresh

I seguenti eventi di sistema sono registrati ciclicamente in una memoria volatile:

i) SYS (system startup, idle time-out, login account authentication) (avvio del sistema, intervallo di inattività, autenticazione di un account utente)

ii) SNTP (network time synchronization) (sincronizzazione dell'ora di rete)

iii) LOG (clear system event log)

iv) PORT (serial port access authentication) (autenticazione accesso porta seriale)

v) DDNS (register dynamic IP address event)

Amministrazione dell'utente

Quando si avvia, il sistema chiede all'utente di digitare la password di accesso. L'amministratore può aggiungere o eliminare un utente semplicemente tramite le pagine web.

Vi sono due tipi di privilegi di accesso:

Nome utente	Password predefinita	Privilegi di accesso
admin	admin	Accesso completo
(definito dall'utente)	(definito dall'utente)	Può accedere solamente alla “Serial Port” (porta seriale) e al “System Status” (Stato del sistema)

La pagina “Access Deny” (Nega accesso) si apre se l'utente non è autorizzato ad accedere alla pagina web.

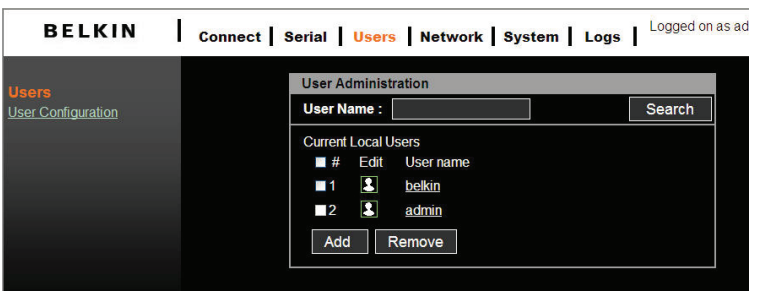
Aggiunta di un utente

Per aggiungere un utente:

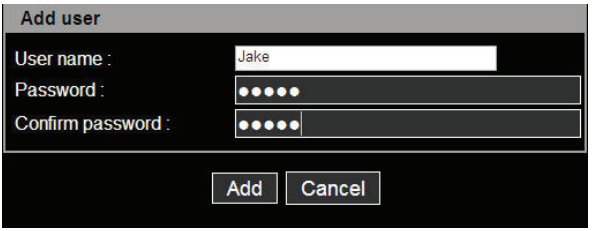
- Controllare gli utenti nella schermata “User administration” (Amministrazione utente).
- Fare clic su "Add" (Aggiungi).
- Digitare il nuovo nome utente e la password.

Linee guida per il nome utente e la password

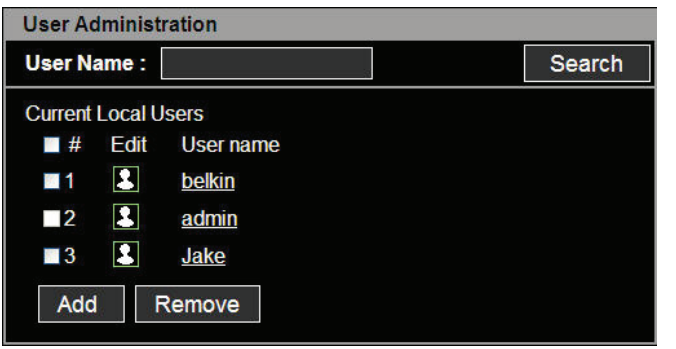
- Il primo carattere del nome utente deve essere una lettera dell'alfabeto.
- La password deve contenere almeno tre caratteri.
- Il nome utente e la password non devono contenere più di 32 caratteri.
- Solo un utente "admin" (amministratore) può accedere alle schede "Network" (rete) e “System administration” (Amministrazione del sistema).



La figura di seguito mostra la schermata "Add User" (Aggiungi utente).



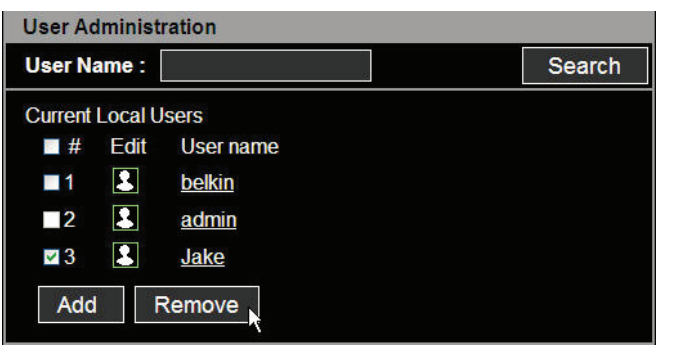
Il nuovo utente appare nell'elenco “User Name” (Nome utente).



Eliminazione di un utente

Per eliminare un utente:

- Controllare gli utenti nella schermata “User administration” (Amministrazione utente).
- Fare clic sul pulsante “Remove” (Elimina)



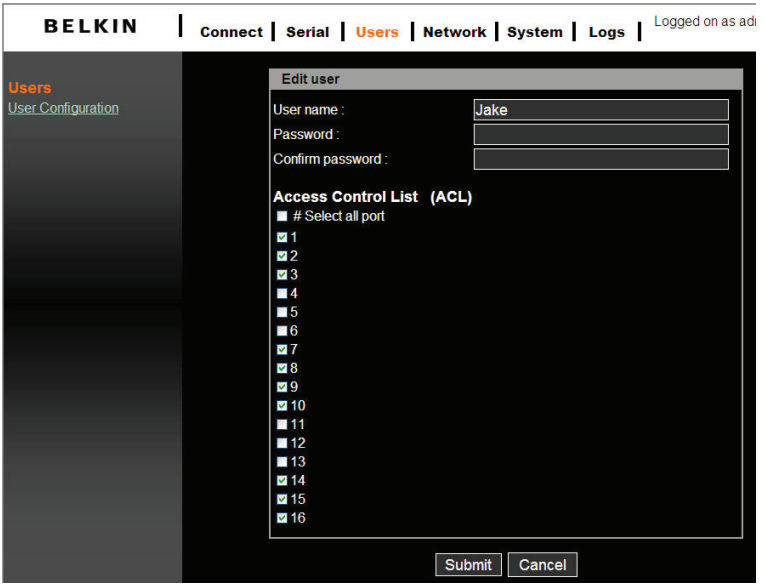
Modifica dell' elenco "Access Control List" (ACL) (lista di controllo degli accessi)

Il Server console è provvisto della protezione ACL (Access Control List) con la quale è possibile specificare l'accesso agli utenti discretamente per ogni porta, anziché per tutte le porte.

Per modificare la protezione ACL:

- Controllare gli utenti nella schermata “User administration” (Amministrazione utente).
- Fare clic sull'icona “Edit” (Modifica).
- Inserire il nome utente e la password.
- Selezionare la porta alla quale si desidera accedere.
- Fare clic su "Submit" (Inoltra).

Una volta impostato un account ACL, gli utenti possono accedere o apportare delle modifiche solo alle porte seriali autorizzate. Gli utenti non sono in grado di visualizzare o configurare porte seriali non autorizzate.



Modifica della password

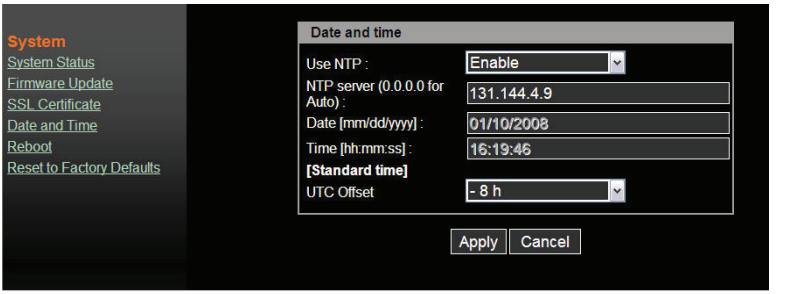
Per cambiare i parametri dell'account utente, aprire la schermata "Edit user" (Modifica utente) selezionando il nome utente nella schermata “User Configuration” (Configurazione utente) e quindi modificare i parametri dell'account utente, come ad esempio aggiungere un utente.

Data e ora (NTP)

Il Server console conserva le informazioni relative alla data e l'ora. Le impostazioni dell'orologio e del calendario sono sottoposte a back up da una batteria interna. L'utente può cambiare la data e l'ora.

Vi sono due opzioni per impostare la data e l'ora. La prima opzione è permettere al server NTP di mantenere le impostazioni relative alla data e all'ora. Se la funzione NTP è attivata, dopo ogni riavvio il server console ottiene le informazioni relative alla data e all'ora dal server NTP, dopodiché ogni ora le allinea a quelle del server. Se il server NTP è impostato su 0.0.0.0, il server console usa automaticamente i server NTP predefiniti. In questo caso, dovrebbe essere collegato dalla rete a Internet. Il secondo metodo consiste nell'impostare la data e l'ora manualmente senza usare il server NTP. In questo caso, le informazioni relative alla data e all'ora rimangono immagazzinate nella batteria di backup interna.

Per convenzione, i meteorologi usano un fuso orario:il Greenwich Mean Time (GMT). Questo orario è anche conosciuto come Universal Time (UTC). È possibile cambiare il fuso orario e la differenza di fuso orario dall'UTC, a seconda della località dove si trova l'utente, in modo tale da impostare il sistema con la data e l'ora esatte, e la differenza di fuso orario dall'UTC. Il valore “Time offset” (differenza di fuso orario) “x” può essere positivo o negativo. Consultare il sito http://time_zone.tripod.com/ su per sapere come cambiare il fuso orario da UTC.



Nota bene:

- Il server console offre la funzione RTC (orologio in tempo reale) alimentata da una batteria al litio (CR2032, 3V). In questo modo, la data e l'ora rimarranno in memoria anche nel caso si verificasse un'interruzione dell'alimentazione.
- Qualora doveste perdere ripetutamente le informazioni relative alla data e l'ora, sostituire
  la batteria.
- Sostituire la batteria CR2032 da 3 Volt solo con una batteria dello stesso tipo o una equivalente, consigliata dal produttore della batteria. Una batteria nuova potrebbe esplodere qualora non fosse installata correttamente. Gettare le batterie usate

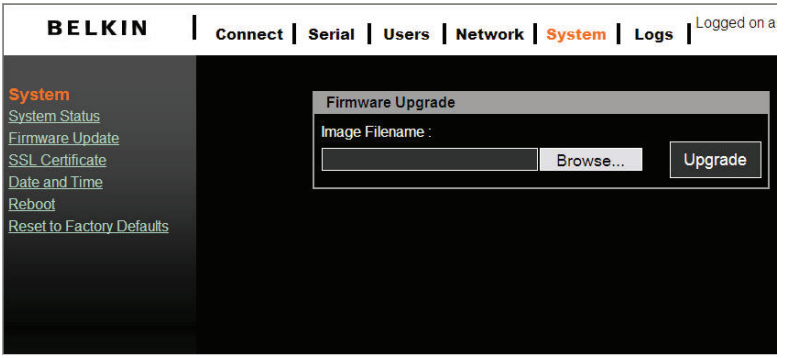
Aggiornamento del firmware

Il Firmware può essere aggiornato semplicemente mediante una pagina web.. Questa sezione descrive il procedimento di aggiornamento.

L'ultima versione del firmware è disponibile su www.belkin.com/support.

Aggiornamento dall' interfaccia web

Consultare la pagina web “System > Firmware Upgrade” (Sistema > Aggiornamento Firmware).

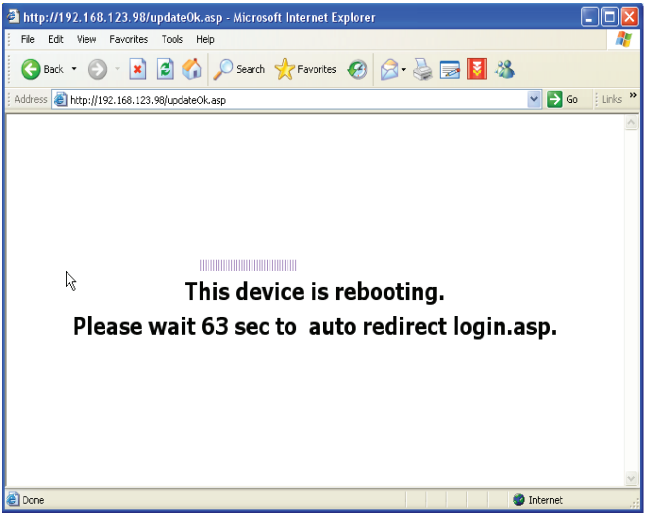


Fare clic su “Browse” (sfoglia) per cercare il file del firmware dalla finestra di Explorer. Navigare nel PC e selezionare il file del firmware. Fare clic su "Open" (Apri) per confermare la propria selezione.

Una volta selezionato il file del firmware corretto, fare clic su “Upgrade” (Aggiorna) per iniziare il procedimento di aggiornamento. L'interfaccia web visualizza la barra di stato che mostrerà lo stato del trasferimento del file. Allo stesso tempo, il LED "port" sul pannello anteriore lampeggia in serie per indicare che è in corso l'aggiornamento.

Avvertenza: NON disconnettere l'alimentazione o il cavo Ethernet durante il procedimento di aggiornamento. Così facendo si potrebbe danneggiare e distruggere l'immagine in memoria.

Il server console si avvierà automaticamente dopo aver effettuato l'aggiornamento, in modo tale da attivare il nuovo firmware. Una volta terminato il conto alla rovescia il browser vi reindirizzerà alla pagina di connessione. Consultare la pagina “System Status” (Stato del sistema) per verificare la versione del firmware e confermare l'aggiornamento.

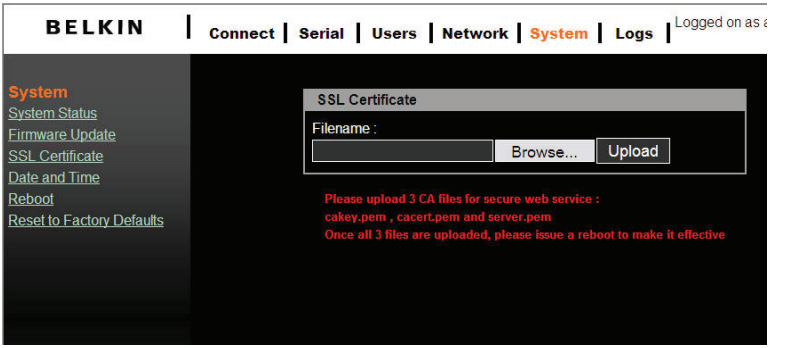


Certificato SSL

Un certificato SSL è un'identificazione digitale che contiene informazioni per attestare che il certificato appartiene ad una determinata persona, organizzazione, server o altra entità riportata nel certificato stesso. Il server console supporta la protezione sicura HTTP (ovvero https) per effettuare delle modifiche alla configurazione via web. Questo certificato sul lato server identifica il server console in modo tale che l'utente possa fidarsi del certificato e apportare delle modifiche alla configurazione senza alcun timore.

Il server console è in grado di caricare file di certificati personalizzati sul server web. La suite del file del certificato include tre file (cacert.pem, cakey.pem e server.pem). Tutti e tre i file del certificato devono essere caricati per completare l'aggiornamento del certificato. L'interfaccia per il caricamento del file è simile all'aggiornamento del firmware.

Una volta caricati tutti i file del certificato, gli utenti devono riavviare manualmente il sistema per fare in modo che il nuovo certificato sia valido.


BELKIN
Connect | Serial | Users | Network | System | Logs | Logged on as
System
System Status
Firmware Update
SSL Certificate
Date and Time
Reboot
Reset to Factory Defaults
SSL Certificate
Filename :
Browse...
Upload
Please upload 3 CA files for secure web service :
cakey.pem , cacert.pem and server.pem
Once all 3 files are uploaded, please issue a reboot to make it effective

Sfogliare i file CA preparati (per preparare correttamente i tre file CA con gli stessi nomi di file assegnati, seguire la procedura descritta nell'allegato E) e caricarli sul server console. Assicurarsi di controllare ogni file prima di caricarlo. Una suite CA falsa potrebbe disattivare la funzione sicura HTTP.

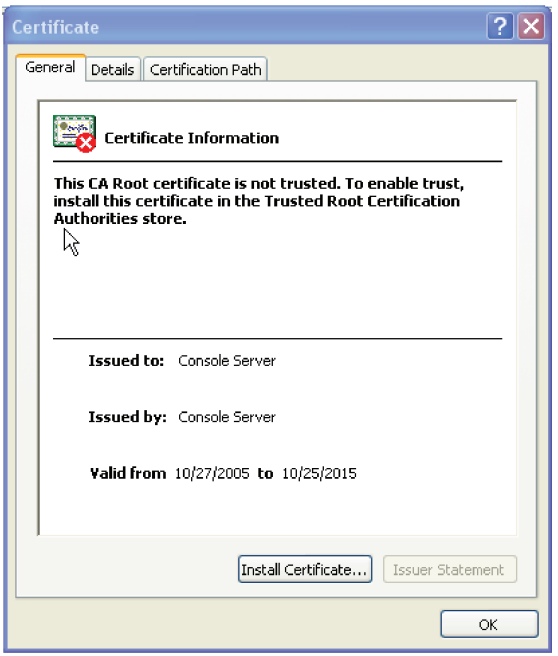
Nota bene:

- Se i file CA fossero danneggiati, gli utenti possono riportarli all'impostazione predefinita andando su “System > Reset to Factory Defaults” (Sistema > Ripristina impostazioni predefinite). In questo modo verranno recuperati i vecchi file CA.
- Poiché la lunghezza del nome del percorso del file CA è limitata (256 caratteri), si consiglia di salvare tutti i file in “C:\upgrade” (C:\aggiornamento) per semplificarne l'amministrazione.
- Nell'allegato E viene illustrato come creare file CA.

Certificato HTTP sicuro

Con la connessione https del browser si avvia un servizio web protetto per il server console (porta di servizio 443). Il browser visualizza un messaggio di avviso per informarvi del certificato. Bisogna accettare il certificato per poter iniziare il servizio web protetto. Gli utenti possono scegliere di visualizzare il certificato (“View Certificate”) e giustificare se il server web collegato sia affidabile.

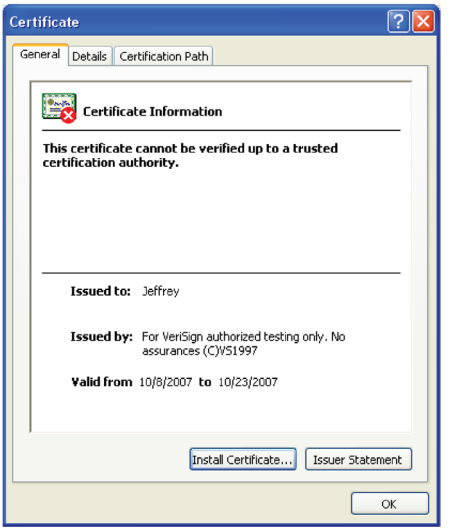
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

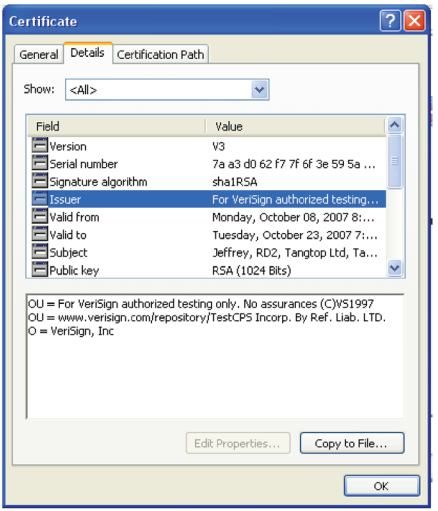

Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Console Server
Issued by: Console Server
Valid from 10/27/2005 to 10/25/2015
Install Certificate...
Issuer Statement
OK

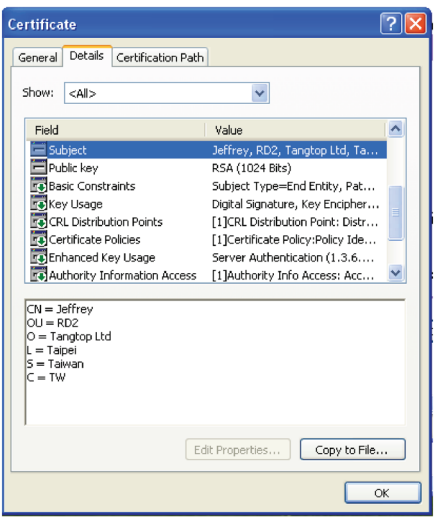
Un altro modo per distinguere una connessione web sicura da una non sicura è vedere se vi sia un lucchetto sul browser (in basso a destra per i browser Internet Explorer). Si può fare doppio clic sul simbolo per verificare le informazioni dettagliate del certificato sul lato server.

Una volta preparata una suite CA di file con chiave pubblica firmata, caricarla dalla pagina “SSL Certificate”. Prima che qualsiasi modifica abbia effetto, è necessario fare riavviare il sistema.

Il seguente esempio illustra un certificato con chiave pubblica e informazioni registrate presso l'autorità preposta ai certificati (VeriSign).




Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
7a a3 d0 62 f7 7f 6f 3e 59 5a ...
Signature algorithm
sha1RSA
Issuer
For VeriSign authorized testing...
Valid from
Monday, October 08, 2007 8:...
Valid to
Tuesday, October 23, 2007 7:...
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
OU = For VeriSign authorized testing only. No assurances (C)V51997
OU = www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.
O = VeriSign, Inc
Edit Properties...
Copy to File...
OK

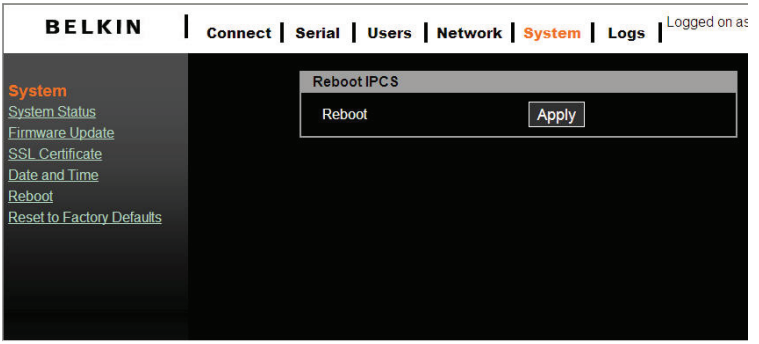

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
Basic Constraints
Subject Type=End Entity, Pat...
Key Usage
Digital Signature, Key Encipher...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Certificate Policies
[1]Certificate Policy:Policy Ide...
Enhanced Key Usage
Server Authentication (1.3.6....
Authority Information Access
[1]Authority Info Access: Acc...
CN = Jeffrey
OU = RD2
O = Tangtop Ltd
L = Taipei
S = Taiwan
C = TW
Edit Properties...
Copy to File...
OK

Ripristino delle impostazioni predefinite

Per ritornare alle impostazioni predefinite, fare clic su "Apply" (Applica).

Riavvio

Dalla rete si può fare in modo che il Server console effettui un riavvio del software. Il riavvio è obbligatorio quando il caricamento del certificato CA è terminato.



Impostazioni predefinite

Nome del server	BelkinSC
DHCP	Abilitato
Indirizzo IP	192.168.2.156
Maschera di rete	255.255.255.0
Gateway	192.168.2.1
Numero di serie	xxxxxxxxx (stampato sul lato inferiore dell'unità)
Indirizzo MAC	xx:xx:xx:xx (stampato sul lato inferiore dell'unità)
Versione e data	Nome e data della versione firmware corrente
Nome utente	admin
Password	admin
Protocollo (seriale)	Telnet
Protocol (web)	HTTP
Filtraggio IP	Disabilitato
Porte seriali --	
Velocità di trasmissione in	9600
baud	8-1
Data/Stop	Nessuno
Parità	Nessuno
Controllo di flusso	0 secondi
Periodo di inattività seriale	Server console
Modalità operativa	**Porta 1:** 4001
Porta TCP	**Porta 2:** 4002
	- - - - - - - -
	Porta 16: 4016

F1D120ea (RJ45F/DB9F DTE)

Adattatore DB9 femmina DTE

Applicazioni: Bay Accelar, Nortel, ecc.
Codice prodotto: F1D120ea - Pacco singolo
F1D120ea8PK - Pacco da 8

Adattatore		
Segnale	RJ45	DB9F
DSR	1	4
DCD	6	
RTS	2	8
GND	3	5
TxD	4	2
RxD	5	3
CTS	7	7
DTR	8	6 1 (DCD)

F1D121ea (RJ45F/DB25F DTE)

Adattatore DB25 femmina DTE

Applicazioni: dispositivi DTE quali PC
Codice prodotto: F1D121ea - Pacco singolo

Adattatore		
Segnale	RJ45	DB25F
DSR	1	20
DCD	6	
RTS	2	5
GND	3	7
TxD	4	3
RxD	5	2
CTS	7	4
DTR	8	6
		8 (DCD)

F1D122ea (RJ45F/DB25M DCE)

Adattatore DB25 maschio DCE

Applicazioni: Modem

Codice prodotto: F1D122ea - Pacco singolo

Adattatore		
Segnale	RJ45	DB25M
DSR	1	6
RTS	2	4
GND	3	5
TxD	4	2
RxD	5	3
DCD	6	1
CTS	7	5
DTR	8	20

F1D123ea (RJ45F/DB25M DTE)

Adattatore DB25 maschio DTE

Applicazioni: Sun SPARC ecc.

Codice prodotto: F1D123ea - Pacco singolo

Adattatore		
Segnale	RJ45	DB25M
DSR	1	20
DCD	6	
RTS	2	5
GND	3	7
TxD	4	3
RxD	5	2
CTS	7	4
DTR	8	6

F1D124ea (RJ45F/RJ45M CISCO)

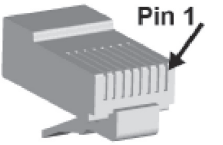
Adattatore RJ45 maschio

Applicazioni: dispositivi Sun

Codice prodotto: F1D124ea - Pacco singolo
F1D124ea8PK - Pacco da 8

Adattatore		
Segnale	RJ45	RJ45M
DSR	1	2
RTS	2	8
GND	3	4
		5
TxD	4	6
RxD	5	3
CTS	7	1
DTR	8	7

Cavo Ethernet RJ45 standard

Connettore	Descrizione	
1	Tx+	
2	Tx-	
3	Rx+	
4	NC	
5	NC	
6	Rx-	
7	NC	
8	NC	

Allegato C: Numeri di porte note TCP/UDP

I numeri di porta sono suddivisi in tre categorie: porte note, porte registrate e porte dinamiche e/o private. Le porte note sono quelle da 0 fino a 1023. Le porte registrate sono quelle dalla 1024 alla 4951. Le porte dinamiche e/o private sono quelle dalla 49152 fino alla 65535.

Le porte note vengono assegnate dalla IANA e, nella maggior parte dei sistemi, possono essere usate solamente da processi di sistemi o programmi effettuati da utenti privilegiati. La tabella riportata di seguito mostra alcuni numeri di porta nota. Per ulteriori informazioni, visitare il sito della IANA: http://www.iana.org/assignments/port-numbers.

Numero porta	Protocollo	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Ora	TCP, UDP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	server BOOTP	UDP
68	client BOOTP	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP (Protocollo per la gestione semplificata della rete)	UDP
443	HTTPS	TCP

BOOTP (Bootstrap Protocol)
Simile al DHCP, ma per reti di dimensioni più piccole. Assegna automaticamente l'indirizzo IP per un periodo di tempo prestabilito.

CHAP (Challenge Handshake Authentication Protocol)
Un protocollo sicuro per collegarsi ad un sistema; è più sicuro del PAP.

DHCP (Protocollo di Configurazione Host Dinamica)
Protocollo Internet per la configurazione automatica dei computer che usano TCP/IP.

DNS (Domain Name Servers)
Un sistema che permette ad un server di rete di tradurre i nomi host testuali in indirizzi IP numerici.

Kerberos
Un protocollo per l'autenticazione di rete che offre una forte autenticazione per applicazioni client/server usando la crittografia a chiave segreta.

LDAP (Lightweight Directory Access Protocol)
Un protocollo per accedere alle informazioni di directory.

NAT (Network Address Translations)
Uno standard Internet che consente a una rete locale (LAN) di usare una grande quantità di indirizzi IP per il traffico interno e un'altra grande quantità di indirizzi per il traffico esterno. Ciò permette ad un'azienda di proteggere la rete interna.

NFS (Network File System)
Un protocollo che permette di condividere file all'interno di una rete. Gli utenti possono visualizzare, immagazzinare ed aggiornare file su un computer remoto. Si può usare l'NFS per memorizzare tutta o una porzione di un file system. Gli utenti possono accedere alla porzione montata con gli stessi privilegi di accesso dell'utente ad ogni file.

NIS (Network Information System)
È un sistema sviluppato dalla Sun Microsystems per la distribuzione di dati di sistema come il nome utente e il nome host tra computer collegati in rete.

NMS (Network Management System)
Il sistema NMS agisce come un server centrale, richiede e riceve informazioni di tipo SNMP da ogni computer che usa il protocollo SNMP.

NTP (Network Time Protocol)
Un protocollo usato per sincronizzare l'orario sui computer e le apparecchiature collegati in rete.

PAP (Password Authentication Protocol)
Un metodo di autenticazione utente nel quale il nome utente e la password vengono trasmessi attraverso una rete e confrontati con coppie di nomi utenti/password presenti in una tabella.

PPP (Point-to-Point Protocol)
Un protocollo per creare e fare eseguire un IP e altri protocolli di rete su un collegamento seriale.

RADIUS (Remote Authentication Dial-In User Service)
Un protocollo di autenticazione e accounting. Permette ai server ad accesso remoto di comunicare con un server centrale per autenticare gli utenti che effettuano il dial-in e i loro permessi di accesso. Una società immagazzina i profili utenti in un database centrale che può essere condiviso da tutti i server remoti.

SNMP (Simple Network Management Protocol)
Un protocollo che gli amministratori di sistema usano per monitorare reti e dispositivi collegati e per rispondere alle domande da altri host di rete.

SMTP (Simple Mail Transfer Protocol)
Protocollo TCP/IP per inviare e-mail tra server.

SSL (Secure Sockets Layer)
Un protocollo che offre i servizi di autenticazione e di crittografia tra un server web e un browser web.

SSH (Secure Shell)
Un protocollo dal trasporto sicuro basato sulla crittografia a chiave pubblica.

TACACS+ (Terminal Access Controller Access Control System)
Un metodo di autenticazione usato nelle reti UNIX. Permette a un server ad accesso remoto di comunicare con un server di autenticazione per determinare se l'utente abbia accesso alla rete.

Telnet
Un protocollo terminale che offre un metodo di facile utilizzo per creare connessioni terminali con un host di rete.

Il server console supporta la configurazione sicura di pagine web (ovvero https). Vi sono due tipi di file certificato per autenticazioni lato server.

- Autofirmato: gli utenti possono creare i file certificato da soli. L'aspetto negativo di ciò è che al client sarà richiesto di accettare un certificato firmato da un'autorità sconosciuta al browser. Generalmente il browser client deve accettare il certificato solo una volta e non gli sarà richiesto nuovamente.
- Firmato da un'autorità di certificazione: Gli utenti creano i file CA e li inviano all'autorità di certificazione (CA) per firmarli. Il vantaggio principale è che al client non verrà richiesto di accettare un certificato.

Gli utenti devono installare il kit di strumenti openSSL prima di creare i file CA precedentemente menzionati. Di seguito è spiegato come generare il certificato per il server web del server console usando openSSL e Linux shell. Il kit di strumenti openSSL può essere scaricato da: http://www.openssl.org/.

1. CA autofirmato:

i) Creazione di una chiave e un certificato X.509:

nel prompt dei comandi di Linux:

openssl req -x509 -newkey rsa:1024 -days 1024 -keyout cakey.pem -out cacert.pem

Le opzioni che possono essere modificate sono:

* l'algoritmo PK può essere cambiato da rsa a dsa e anche la lunghezza della chiave in bit (512, 1024, 2048, 4096).

* il periodo di tempo di validità del certificato; impostato su 1024 giorni, ovvero meno di tre anni.

È possibile impostare la data di inizio/fine della validità del certificato. Vi verrà richiesto due volte di inserire la frase di accesso PEM per la chiave e quindi inserire le informazioni necessarie per il certificato:

Di seguito un esempio di prompt:

Nazione	<USA>
Stato o provincia	<Propriostato>
Città/Località	<Ancoraggio>
Organizzazione	<Nome della società>
Unità organizzativa Prolix	<R & D>
Nome comune (NOME HOST DEL SERVER)	<IPCS>
Indirizzo e-mail dell'amministratore del server	<tu@tuodominio.com>

ii) Frase di accesso Strip:

openssl rsa -in cakey.pem -out cakey-nopassword.pem

iii) Combina la chiave e i file certificato X.509 nel server.perm:

cat cakey-nopassword.pem cacert.pem > server.pem

iv) Collezionare tutti e 3 i file PEM e prepararli per caricarli sul server IPCS:

server.pem , cacert.pem , cakey.pem

2. Firmato da un'autorità di certificazione fidata:

i) Preparare la chiave privata **cakey.pem:**

openssl genrsa –des3 –out cakey.pem 1024

significato dei parametri:

genrsa : genera una chiave privata RSA

des3 : certificato crittografato da DES3

1024 : la dimensione della chiave è di 1024 bit

ii) Preparazione di sottoscrizione del certificato:

openssl req –new –key cakey.pem –out server.csr

Il kit di strumenti openSSL guiderà l'utente nella compilazione di un modulo di registrazione. Una volta completato, gli utenti possono inviare il file CSR a www.verisign.com per dei test o consultare il sito http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp (con sede a Taiwan) per richiedere un certificato firmato. Dopo aver ottenuto il certificato nominare il file “cacert.pem”.

iii) Frase di accesso Strip:

openssl rsa –in cakey.pem –out cakey-nopassword.pem

iv) Combina la chiave e i file certificato X.509 nel server.perm:

cat cakey-nopassword.pem cacert.pem > server.pem

v) Collezionare tutti e 3 i file PEM per il caricamento:

server.pem , cacert.pem , cakey.pem

Dichiarazione FCC

DICHIARAZIONE DI CONFORMITÀ CON LE LEGGI FCC PER LA COMPATIBILITÀ ELETTROMAGNETICA

Noi sottoscritti, Belkin International, Inc., con sede al 501 West Walnut Street, Compton, CA 90220, dichiariamo sotto la nostra piena responsabilità che il prodotto:
F1DP116S, al quale questa dichiarazione fa riferimento:

è conforme alla Parte 15 delle norme FCC. Le condizioni per il funzionamento sono le due seguenti:

(1) il dispositivo non deve causare interferenze dannose e (2) il dispositivo deve accettare qualsiasi interferenza ricevuta, comprese eventuali interferenze che possano causare un funzionamento anomalo.

Questa attrezzatura è stata testata ed è risultata conforme ai limiti previsti per le periferiche digitali di classe A, in conformità alla Sezione 15 delle norme FCC. Questi limiti sono stati designati per fornire una protezione ragionevole da interferenze dannose, quando l'apparecchio viene usato in un ambiente commerciale. Questo apparecchio genera, utilizza e può irradiare energia a radiofrequenza e, se non viene installato e impiegato seguendo le istruzioni, può causare interferenze distruttive per le comunicazioni radio. Questo apparecchio può causare interferenze dannose in ambienti domestici. In questo caso l'utente deve provvedere ad eliminare l'interferenza a spese proprie.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministére des Communications du Canada.

Dichiarazione di conformità CE

Noi sottoscritti, Belkin International, Inc.,dichiariamo sotto la nostra piena responsabilità che il prodotto F1DP116S, al quale questa dichiarazione fa riferimento, è realizzato in conformità allo Standard sulle Emissioni EN55022 Classe A e alla Norma di Immunità EN55024, nonché agli standard LVP EN61000-3-2 e EN61000-3-3.

ICES

Questo apparecchio digitale di classe A è conforme allo standard canadese ICES-003. Cet appareil numérique de la classe A conforme á la norme NMB-003 du Canada.

Garanzia limitata di 2 anni sul prodotto Belkin International, Inc.

Oggetto della garanzia.

Belkin International, Inc. ("Belkin") garantisce all'acquirente di questo prodotto Belkin che tale prodotto è esente da difetti di progettazione, montaggio, materiale e lavorazione.

Periodo di copertura della garanzia.

Belkin garantisce il prodotto Belkin per due anni.

Risoluzione di eventuali problemi.
Garanzia sul prodotto.
Belkin provvederà a riparare o sostituire gratuitamente, a propria discrezione, qualsiasi prodotto che dovesse risultare difettoso (escluse le spese di trasporto).

Condizioni non coperte dalla garanzia.
Tutte le garanzie di cui sopra saranno rese nulle qualora il prodotto Belkin non fosse fornito alla Belkin per essere sottoposto alle necessarie verifiche dietro espressa richiesta di Belkin e a spese del cliente, oppure nel caso in cui la Belkin dovesse stabilire che il prodotto non è stato correttamente installato o che sia stato in qualche modo alterato o manomesso.
La garanzia sul prodotto Belkin non copre danni da imputarsi a calamità naturali, tra cui allagamenti, fulmini, terremoti, guerre, atti di vandalismo, furti, usura, erosione, assottigliamento, obsolescenza, abusi, danni dovuti ad interferenze di bassa tensione (tra cui parziali oscuramenti o abbassamenti di tensione), programmazione non autorizzata oppure modifiche o alterazioni all'apparecchiatura dell'impianto.

Come ottenere l'assistenza.
Per usufruire dell'assistenza per il proprio prodotto Belkin, è necessario:

1. Contattare la Belkin International, Inc. all'indirizzo 501 W. Walnut St., Compton CA 90220, att.: Customer Service oppure chiamare il numero (800)-223-5546, entro 15 giorni dall'evento. Vi sarà richiesto di fornire le seguenti informazioni:
    a. Il codice del prodotto Belkin.
    b. Il luogo di acquisto del prodotto.
    c. La data di acquisto del prodotto.
    d. Copia della ricevuta originale.

2. Il rappresentante del Servizio Clienti Belkin vi spiegherà come inviare la ricevuta e il prodotto Belkin e come procedere con il reclamo.

Belkin si riserva il diritto di riesaminare il prodotto Belkin danneggiato. Tutte le spese di spedizione per il prodotto Belkin restituito alla Belkin sono a carico dell'acquirente. Se Belkin dovesse ritenere, a propria discrezione, che inviare l'apparecchio danneggiato non sia conveniente, Belkin potrà decidere, a propria discrezione, di farlo ispezionare e determinare il costo della riparazione presso una struttura diversa dalla propria. L'acquirente si farà carico di eventuali spese di spedizione, causate dal rinvio e dalla ricezione dell'apparecchio dopo l'ispezione. Eventuali apparecchi danneggiati dovranno essere mantenuti disponibili per eventuali verifiche fino alla risoluzione della richiesta di indennizzo. Al raggiungimento dell'accordo, Belkin si riserva il diritto di essere surrogata da eventuali polizze assicurative dell'acquirente.

Cosa stabilisce la legge riguardo alla garanzia.
LA PRESENTE GARANZIA COSTITUISCE L'UNICA GARANZIA DI BELKIN. SI ESCLUDE QUALSIASI GARANZIA IMPLICITA, DI COMMERCIABILITÀ E DI IDONEITÀ PER SCOPI PARTICOLARI CHE VADA OLTRE LA DURATA DELLA PRESENTE GARANZIA ESPLICITA SCRITTA

Alcune giurisdizioni non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali, pertanto i limiti di esclusione di cui sopra potrebbero non essere applicabili.

IN NESSUN CASO BELKIN POTRÀ ESSERE CONSIDERATA RESPONSABILE DI ALCUN DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIFICO O DANNI MULTIPLI TRA I QUALI, MA NON LIMITATI A, EVENTUALI DANNI DI MANCATI AFFARI O MANCATO GUADAGNO DERIVATI DALLA VENDITA O UTILIZZO DI QUALSIASI PRODOTTO BELKIN, ANCHE NEL CASO IN CUI SI FOSSE STATI INFORMATI DELLA POSSIBILITÀ DI TALI DANNI.

Questa garanzia consente di godere di diritti legali specifici e di eventuali altri diritti che possono variare di stato in stato. Alcune giurisdizioni non consentono l'esclusione o la limitazione delle garanzie implicite o della responsabilità per i danni accidentali o altri danni, pertanto i limiti di esclusione di cui sopra potrebbero non essere applicabili.

BELKIN®

Server console seriale OmniView®

Assistenza tecnica gratuita*

Per maggiori informazioni sull'assistenza tecnica, visitare il nostro sito web www.belkin.it nell'area centro assistenza. Per contattare telefonicamente il servizio di assistenza tecnica, chiamare uno dei seguenti numeri*.

*Si applicano le tariffe locali

Paese	Numero	Indirizzo Internet
AUSTRIA	0820 200766	http://www.belkin.com/uk/support/
BELGIO	07 07 00 073	http://www.belkin.com/nl/support/
REPUBBLICA CECA	239 000 406	http://www.belkin.com/uk/support/
DANIMARCA	701 22 403	http://www.belkin.com/uk/support/
FINLANDIA	00800 - 22 35 54 60	http://www.belkin.com/uk/support/
FRANCIA	08 - 25 54 00 26	http://www.belkin.com/fr/support/
GERMANIA	0180 - 500 57 09	http://www.belkin.com/de/support/
GRECIA	00800 - 44 14 23 90	http://www.belkin.com/uk/support/
UNGHERIA	06 - 17 77 49 06	http://www.belkin.com/uk/support/
ISLANDA	800 8534	http://www.belkin.com/uk/support/
IRLANDA	0818 55 50 06	http://www.belkin.com/uk/support/
ITALIA	02 - 69 43 02 51	http://www.belkin.com/it/ support
LUSSEMBURGO	34 20 80 85 60	http://www.belkin.com/uk/support/
PAESI BASSI	0900 - 040 07 90 € 0,10 al	http://www.belkin.com/nl/support/
NORVEGIA	81 50 0287	http://www.belkin.com/uk/support/
POLONIA	00800 - 441 17 37	http://www.belkin.com/uk/support/
PORTOGALLO	707 200 676	http://www.belkin.com/uk/support/
RUSSIA	495 580 9541	http://www.belkin.com/uk/support/
SUDAFRICA	0800 - 99 15 21	http://www.belkin.com/uk/support/
SPAGNA	902 - 02 43 66	http://www.belkin.com/es/support/
SVEZIA	07 - 71 40 04 53	http://www.belkin.com/uk/support/
SVIZZERA	08 - 48 00 02 19	http://www.belkin.com/uk/support/
REGNO UNITO	0845 - 607 77 87	http://www.belkin.com/uk/support/
ALTRI PAESI	+44 - 1933 35 20 00	

BELKIN®

www.belkin.com

Belkin Ltd.
Express Business Park
Shipton Way, Rushden
NN10 6GL, Regno Unito

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk
Paesi Bassi

Belkin GmbH
Hanebergstrasse 2
80637 Monaco di Baviera
Germania

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt
Francia

Belkin Iberia
Avda. Cerro del Aguila 3
28700 San Sebastián de los Reyes
Spagna

Belkin Svezia
Knarrarnäsgatan 7
164 40 Kista
Svezia

© 2008 Belkin International, Inc. Tutti i diritti riservati. Tutti i nomi commerciali sono marchi registrati dei rispettivi produttori indicati. Windows è un marchio commerciale o un marchio registrato della Microsoft Corporation negli Stati Uniti e/o in altri Paesi.

P75598ea